SERVIS IP-KVM

FW-D シリーズ

取扱説明書

02 版

改版履歴

版数	発行年月日	内容
01	2012/4/18	初版作成
02	2013/08/29	ファームウェアバージョン 1.18.0.22011 に合わせて内容を更新。 Java Runtime Environment のサポート情報を追記。 既知の不具合について記載。 ハイセイフティ用途の定義を更新。

Ethernet およびイーサネットは、富士ゼロックス株式会社の登録商標です。

Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標または商標です。

Microsoft、Windows、Windows Server は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

Oracle と Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。
Red Hat、RPM および Red Hat をベースとしたすべての商標とロゴは、Red Hat, Inc.の米国およびその他の国における登録商標あるいは商標です。

SERVIS は富士通コンポーネント株式会社の登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標である場合があります。
なお、本文中では ® および ™ マークは省略しています。

はじめに

このたびは、SERVIS IP-KVM FW-D シリーズ （以降、本製品と略します）をお買い上げいただきまして誠にありがとうございます。

本製品は、ネットワークを経由した遠隔地からターゲットデバイス（PC、サーバー類）のキーボード、ビデオ、マウス（KVM）操作、また RS-232C シリアルデバイスの操作を可能にするための装置です。
本製品にはモデルにより、8、16、32 個のターゲットデバイス接続ポートを持ち、対応する台数のターゲットデバイスを接続することができます。
また、ネットワーク上のデータの暗号化（SSL, SSH）機能を持っているため、セキュアなネットワーク通信を可能にします。
その他、バーチャルメディアという機能を持っており、リモート端末に接続されているディスクドライブをターゲットデバイス側に認識させることができ、リモート端末とターゲットデバイス間のファイル転送などを容易にします。
また、本製品は 2 つの独立した電源構成（リダンダント）をもち、電源の冗長化が可能になります。これにより、電源ケーブルの断線・接続不良、本体の電源ユニットの故障などの障害による機能停止を防ぎます。

本書では、セットアップ、基本操作方法、各種機能について説明します。

本書について

この取扱説明書（以降、本書と略します）は、本製品を安全に正しくお使いいただくために守っていただきたい重要な情報が記載されています。
本製品をお使いになる前に本書をよくお読みになり、本製品を正しくお使いください。
また、本書は本製品の使用中いつでも参照できるよう、大切に保管してください。
弊社は、使用者および周囲の方々の身体や財産に被害を及ぼすことなく安全に使っていただくために、細心の注意を払っております。本製品をご使用になる際は、本書の説明に従ってください。

本製品および本書の内容については、改良のために予告なく変更することがあります。
本製品および本書の内容について、不明な点やお気づきの点がございましたら、弊社保守サービス係までご連絡願います。

ご使用上の注意

本製品として提供される取扱説明書(本書)、装置本体は、お客様の責任でご使用ください。本製品の使用によって発生する損失やデータの損失については、富士通コンポーネント株式会社では一切責任を負いかねます。また、本製品の障害の保証範囲はどのような場合でも、本製品の代金としてお支払いいただいた金額を超えることはありません。あらかじめご了承ください。

輸出管理規制について

本製品が「外国為替および外国貿易管理法」に基づき規制されている貨物または技術に該当する場合は、当該製品を輸出するに際して司法に基づく許可が必要になります。したがいまして、国外に持ち出す場合には必ず日本国政府の輸出許可申請など必要な手続きをお取りください。

電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づく クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には、使用者が適切な対策を講じるよう要求されることがあります。

ハイセイフティ用途について

本製品は、一般事務用、パーソナル用、家庭用、通常の産業用等の一般的用途を想定して設計・製造されているものであり、(1)原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御などの、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途ならびに(2)海底中継器、宇宙衛星など、極めて高度な信頼性が要求される用途 (以下「ハイセイフティ用途」という) に使用されるよう設計・製造されたものではございません。
お客様は当該ハイセイフティ用途に要する安全性ならびに信頼性を確保する措置を施すことなく、本製品を使用しないでください。また、お客様がハイセイフティ用途に本製品を使用したことにより発生する、お客様又は第三者からの如何なる請求又は損害賠償に対しても、富士通コンポーネント株式会社およびその関連会社は一切責任を負いかねます。

本製品の廃棄時の取り扱いについて

本製品は金属、プラスチック部品を使用しています。廃棄するときは、各自治体の指示に従ってください。

本書の表記について

本書の表記ルールについて以下に示します。

書体または記号	意味
AaBbCc123	画面上の本製品あるいは接続機器からの出力を表します。
AaBbCc123	コマンドや設定ファイルにおいてユーザーが入力する文字を表します。
Enter↵	ユーザーによる Enter キー入力を表します。
🕮 参照	参照する Chapter, 項目, ページ数を表します。
重要	本製品をご使用になる上で、気を付けていただきたい点を示しています。

目次

Chapter 1 - 製品概要

本製品の概要、およびセットアップを行う上で必要な情報を説明しています。作業を始める前にお読みください。

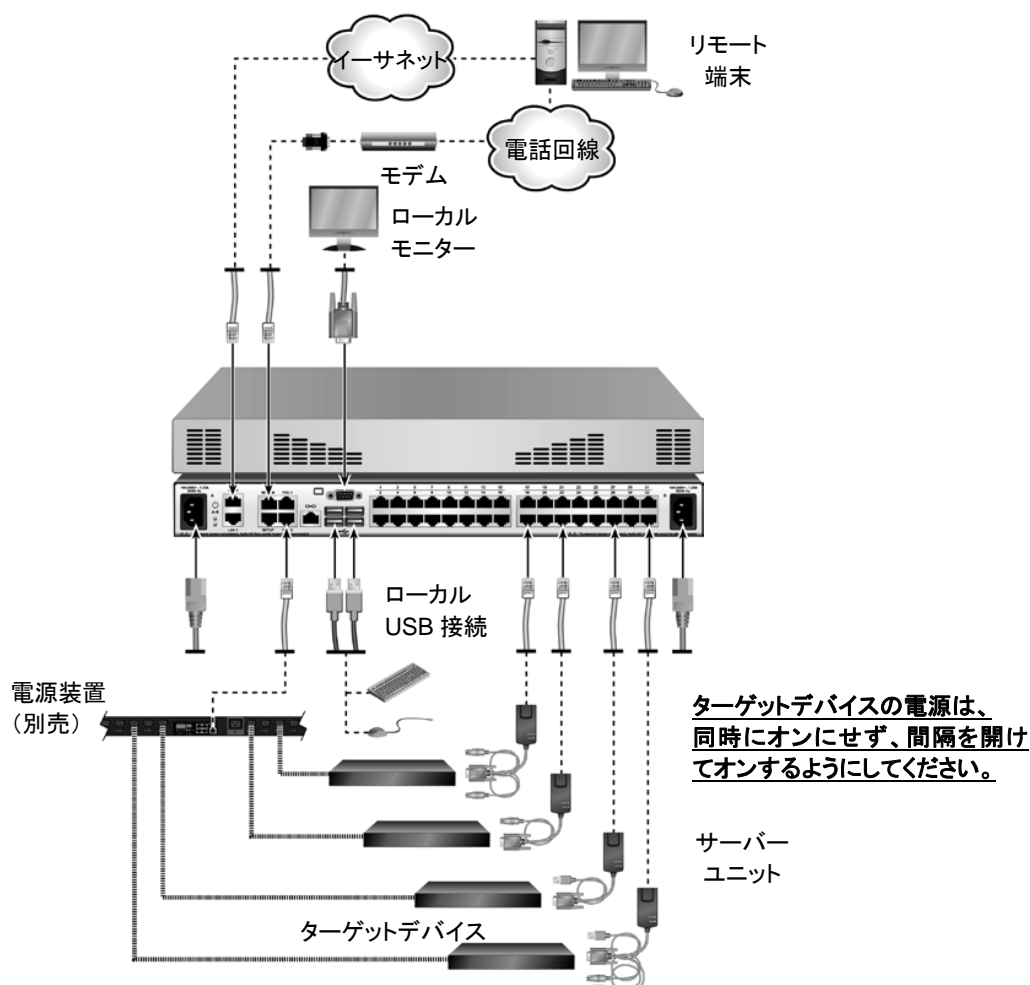
本章の内容

1.1.　本製品の概要

本製品は、ネットワークを経由した遠隔地からターゲットデバイス（PC、サーバー類）のキーボード、ビデオ、マウス（KVM）操作、また RS-232C シリアルデバイスの操作を可能にするための装置です。

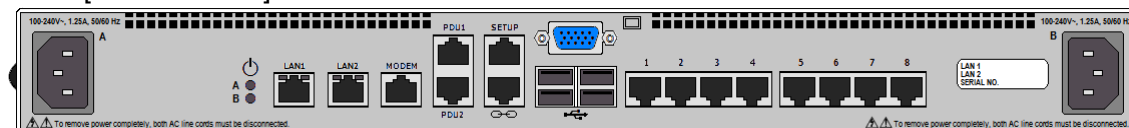
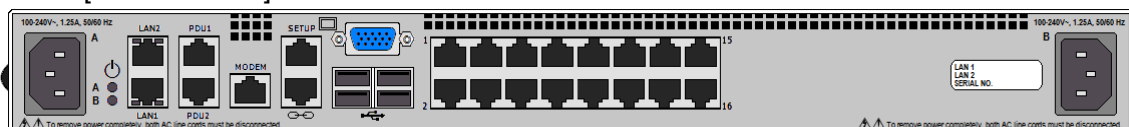
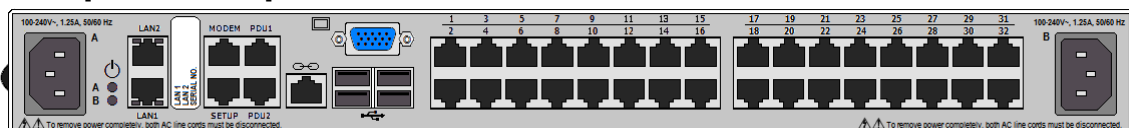
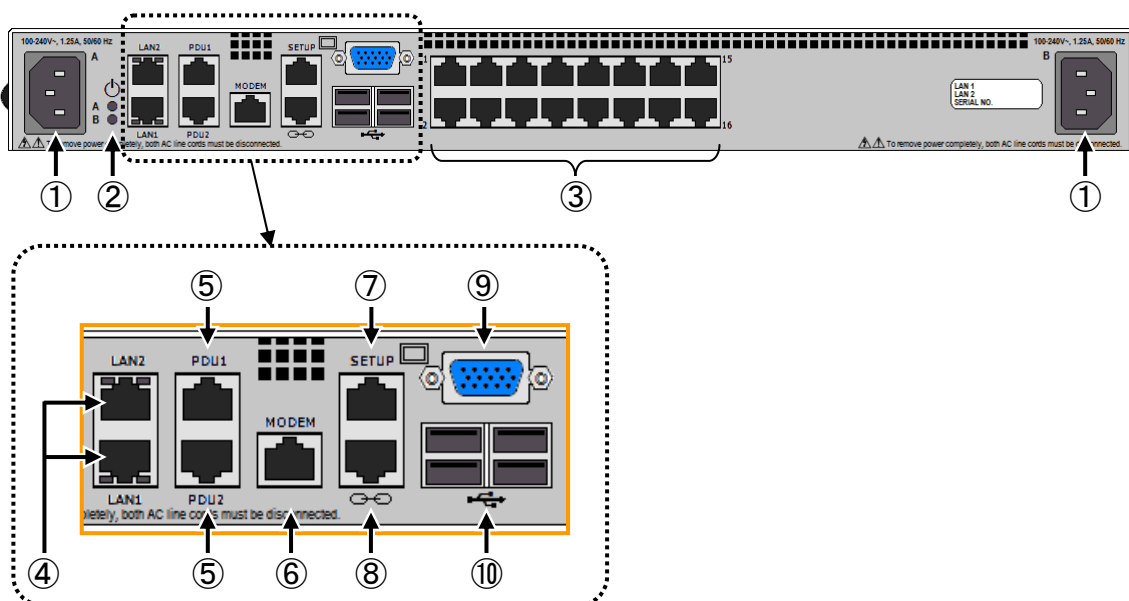
本製品には、下記の 3 種類の型格があり、ターゲットポート数、リモートユーザー数によって、ご利用の製品を選択することができます。ターゲットポート数とは、本装置に接続することができるターゲットデバイスの接続ポート数を意味します。
リモートユーザー数とは、ネットワーク上のリモート端末から同時にターゲットデバイスへアクセスすることが可能な最大ユーザー数を意味します。
また、本装置にはローカルのキーボード、モニター、マウスのコネクタがあり、そちらから 1 ユーザーのみ（ローカルユーザーと呼びます）本装置の設定およびターゲットデバイスを操作することができます。

型格	リモートユーザー数	ローカルユーザー数	ターゲットポート数
FW-D1108NP	1	1	8
FW-D2116NP	2	1	16
FW-D8132NP	8	1	32

また、イーサネット接続が利用できない場合でも、V34、V.90、V.92 対応モデムをサポートするモデムポートにより、電話回線から本製品へのアクセスが可能です。

1.2. 本体各部の名称と機能

前面部（共通）

背面部

[FW-D1108NP]

[FW-D2116NP]

[FW-D8132NP]

[各コネクタ／ポートについて] (FW-D2116NP の例)

① 電源インレット

添付の電源ケーブルを接続します。
本製品は、電源ケーブルを 2 本まで接続することができ、冗長構成が可能です。
左端のインレットが A、右端のインレットが B になります。

② 電源 LED

電源インレット A, B それぞれの電源供給状態を示します。
電源供給されている場合、緑色点灯します。

③ ターゲットポート

ターゲットデバイスに接続するサーバーユニットと接続するためのポートです。
コネクタ形状は RJ45 モジュラージャックです。ケーブルは、市販の Cat5e ストレートケーブルを使用します。

④ LAN1, 2 ポート

10BASE-T/100BASE-TX/1000BASE-T に対応した Ethernet 接続用ソケットです。
コネクタ形状は RJ45 モジュラージャックです。ケーブルは、Cat5e ストレートケーブルを使用します。

⑤ PDU1, 2 ポート

オプション（別売）の電源装置の IN ポートと接続します。
コネクタ形状は RJ45 モジュラージャックです。ケーブルは、Cat5e ストレートケーブルを使用します。
🕮 参照 1.8 電源装置との接続（14 ページ）

⑥ MODEM ポート

公衆回線アクセス用で、添付の変換アダプタおよびケーブルを用いて、モデムと接続します。コネクタ形状は RJ45 モジュラージャックです。
🕮 参照 1.7 モデム接続（13 ページ）

⑦ SETUP ポート

シリアルコンソール接続用で、初期導入時にネットワークの設定などを行います。
コネクタ形状は RJ45 モジュラージャックです。添付の変換アダプタおよびケーブルを用いて、シリアルコンソール端末と接続します。
🕮 参照 Chapter 5 - シリアルコンソール（223 ページ）

⑧ カスケードポート

本装置のカスケード接続用のポートです。
コネクタ形状は RJ45 モジュラージャックです。ケーブルは、Cat5e ストレートケーブルを使用します。
🕮 参照 1.6 カスケード接続（12 ページ）

⑨ ローカル ビデオ ポート

ローカルで操作するためのビデオモニタを接続します。
コネクタ形状は D-Sub 15pin(DE15) です。

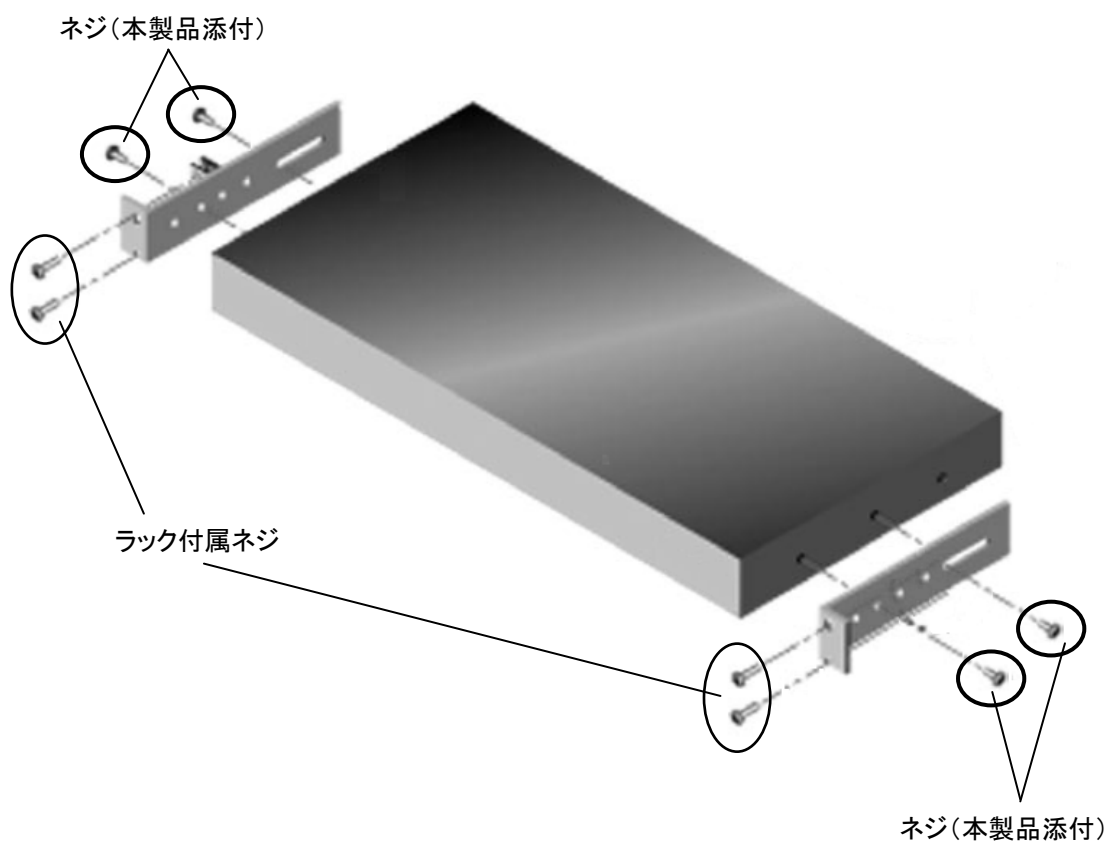
⑩ ローカル USB ポート

ローカルで操作するための USB キーボード、マウス あるいは、バーチャルメディアとしてマッピングさせる USB ストレージや USB CD/DVD-ROM ドライブなどを接続します。 コネクタ形状は USB タイプ A で 4 個まで接続可能です。

1.3. ラックマウント

添付のラックマウントキットを製品本体に取り付けることにより、EIA 規格の 19 インチラックに取り付けることができます。

[FW-D1108NP, FW-D2116NP の場合]

- 本体側面の左右 4 ヶ所のネジを取り外します。
- 本体側面に添付の取付け金具を合わせ、添付のネジでしっかりとネジ締めします。
- ラックに付属のネジを用いて、19 インチラックの任意の位置に固定します。

[FW-D8132NP の場合]

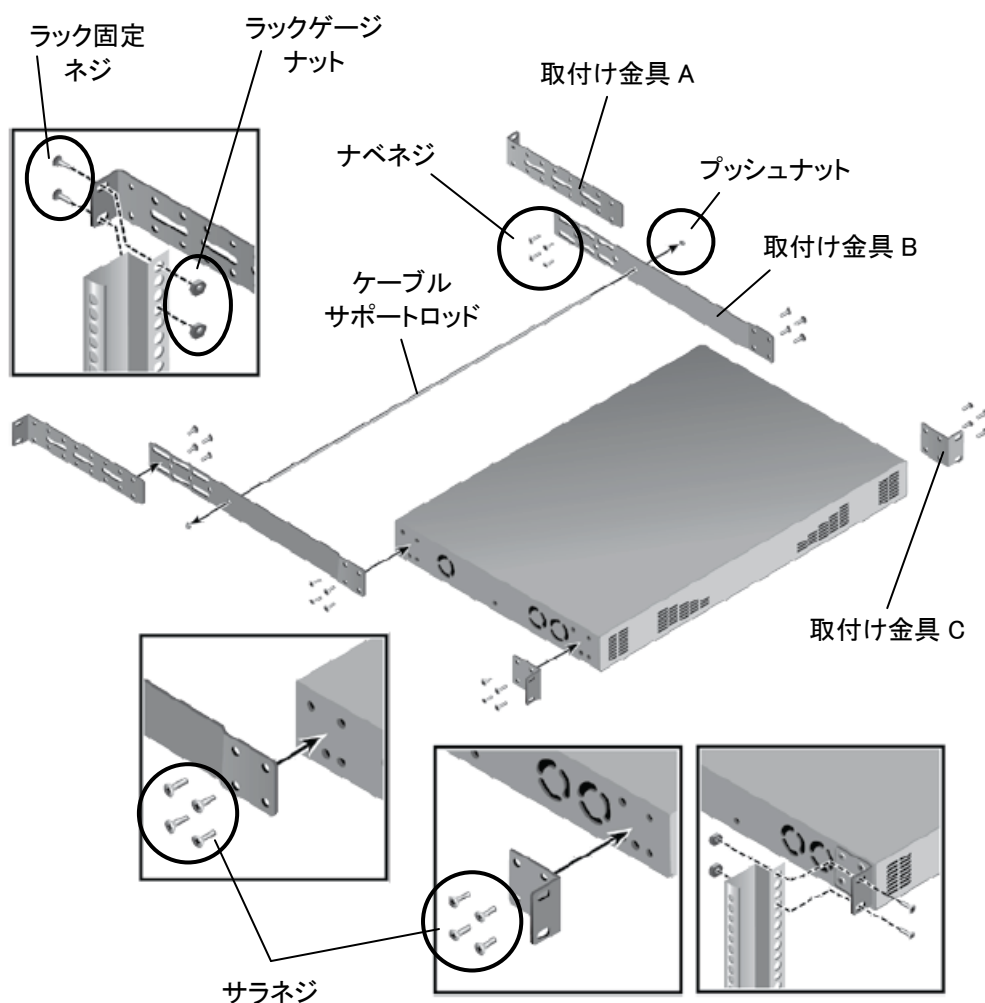
FW-D8132NP のフランジキットには、以下の内容物が含まれています。

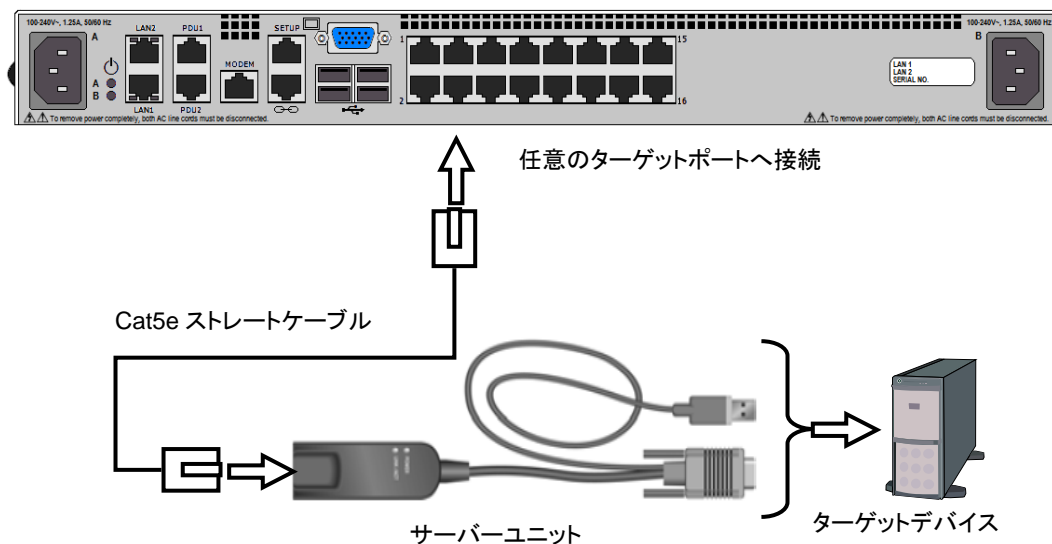
- 取付け金具 A …2 個
- 取付け金具 B …2 個
- 取付け金具 C …2 個
- サラネジ …16 個
- ナベネジ …8 個
- ラックゲージナット …8 個
- ラック固定用ネジ …8 個
- ケーブルサポートロッド …1 個
- プッシュナット …2 個

下の図のようにフランジキットを取り付けます。

- サラネジを用いて、取付け金具 B を本装置に取り付けます。
- サラネジを用いて、取付け金具 C を本装置に取り付けます。
- ナベネジを用いて、取付け金具 B と取付け金具 A を接続します。
- ラックゲージナットとラック固定ネジを用いて、任意のラック位置に本装置を設置します。
- ケーブルサポートロッドを延長金具の任意の位置に通し、プッシュナットで留めます。

1

製品概要

1.4. サーバーユニット

製品本体とターゲットデバイスの接続を行うためには、サーバーユニットという専用のアダプタが必要となります。下のような形状をしており、PS/2 あるいは USB、ビデオコネクタをターゲットデバイスに接続し、RJ45 側のコネクタに Cat5e ストレートケーブルを接続して製品本体のターゲットポートと接続します。接続が完了してから、ターゲットデバイスの電源を投入してください。

サーバーユニットには以下の 4 種類のモデルがあり、接続コネクタ形状、機能によって選択してご利用いただくことができます。

- FW-DSM02/USB-L

  キーボード、マウス、モニターが接続できる PC やサーバーに対して接続するモデルで、ターゲットデバイスのキーボード、マウスポートに USB コネクタを用いて接続します。
  ターゲットデバイスの解像度は等倍表示で 1024x768(75Hz)まで、縮小表示で 1280x1024（75Hz）まで表示可能です。
  また、バーチャルメディア機能を使用することができます。

- FW-DSM03/VMC

キーボード、マウス、モニターが接続できる PC やサーバーに対して接続するモデルで、ターゲットデバイスのキーボード、マウスポートに USB コネクタを用いて接続します。
ターゲットデバイスの解像度は 1600x1200（60Hz）または 1680x1050（60Hz）まで等倍表示可能です。
また、バーチャルメディア機能を使用することができます。

重要

このサーバーユニットはスマートカードリーダ機能を持っておりますが、本製品ではサポートしておりませんので、予めご了承下さい。

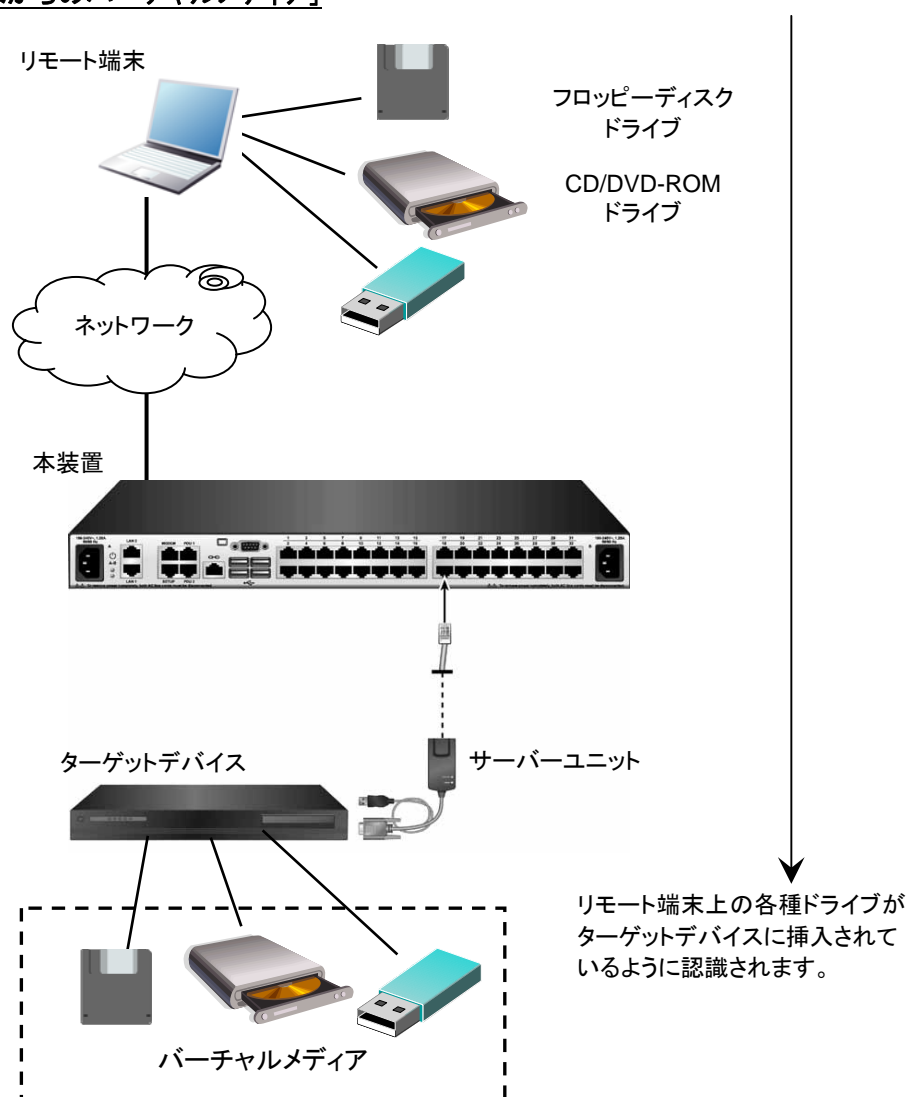
- FW-DSM03/SRL

スイッチングハブやルーターなどの RS232C ポートを持つシリアルデバイスに対して接続するモデルで、RJ45 コネクタ あるいは D-sub9 ピンコネクタ（RJ45⇔D-sub9 変換アダプタ同梱）によって接続します。
参照 4.20 シリアルデバイスの操作（213 ページ）

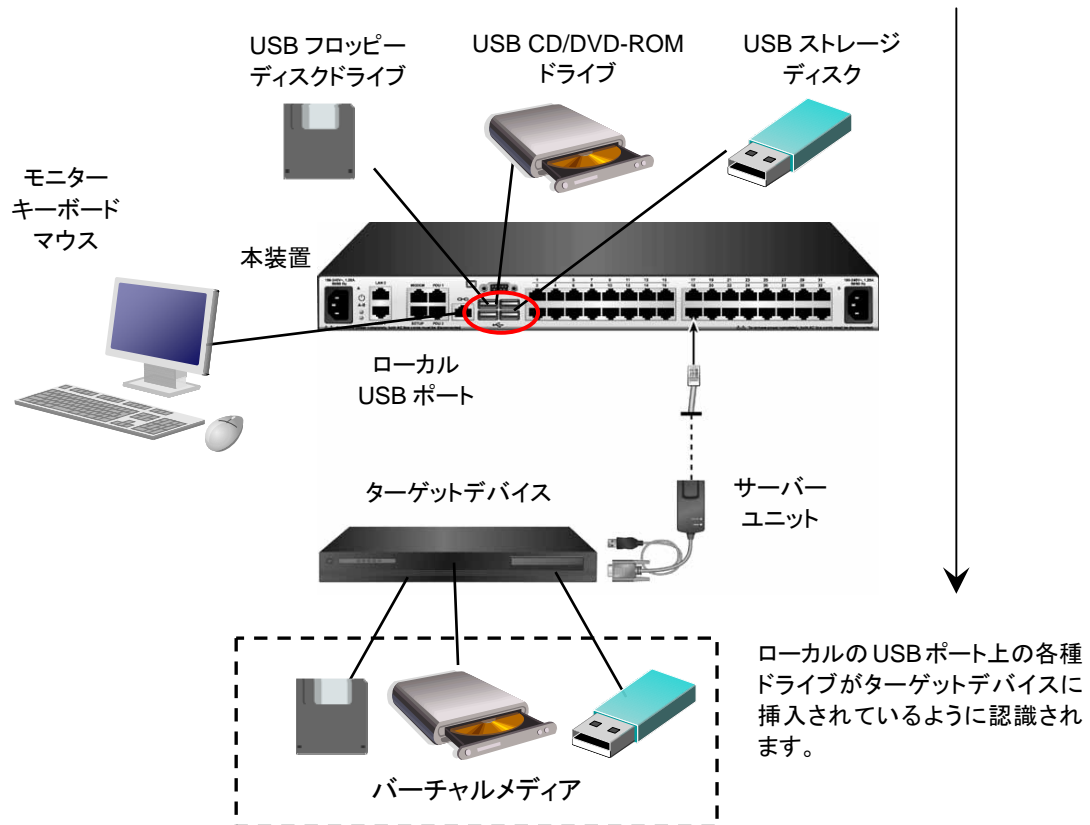
1.5. バーチャルメディア機能

PC あるいはサーバーをターゲットデバイスとするサーバーユニット（FW-DSM02/PS2-M, FW-DSM02/USB-L, FW-DSM03/VMC）には、バーチャルメディアという機能があります。

リモート端末からのターゲットデバイスの操作において、リモート端末上に接続されたフロッピーディスク、CD/DVD-ROM、USB ストレージがあたかもターゲットデバイスに直接接続されているかのように、ターゲットデバイスにマッピングさせることができるものです。
これにより、リモート端末側とターゲットデバイス側のデータの送受信が容易になり、ターゲットデバイスへの OS インストールやデータのバックアップ・複製などシステム管理に関わる作業を効率よく行うことが可能となります。

［リモート端末からのバーチャルメディア］

操作方法の詳細については、下記をご参照ください。
📖 参照 4.13 バーチャルメディア （190 ページ）

[ローカルからのバーチャルメディア]

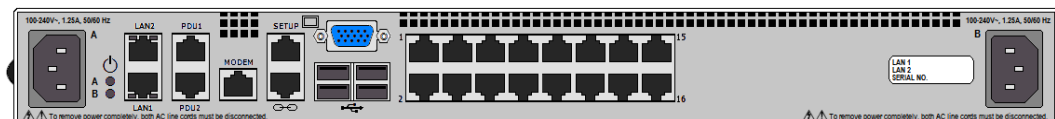
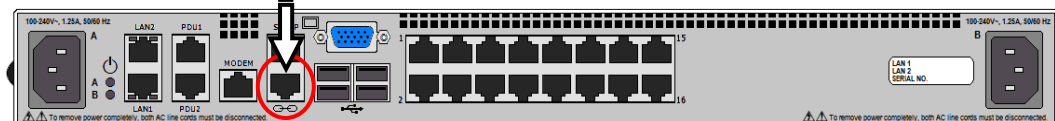
また、装置本体のローカル USB ポートに上に接続された USB フロッピーディスク、USB CD/DVD-ROM、USB ストレージについても同様にターゲットデバイスにマッピングさせることができます。

操作方法の詳細については、下記をご参照ください。
参照 4.13 バーチャルメディア（190 ページ）

1.6. カスケード接続

カスケード接続として、製品本体に 1 段さらに本製品を接続することができます。スレーブ装置側にさらに(2 段目)カスケード接続することはできません。
割り当てる IP アドレスが足りない場合などに本接続構成をご利用ください。(※幾つか制限事項があります。)

ターゲットポートが 32 ポートあるモデル(FW-D8132NP)を用いてカスケード接続することにより、最大構成でターゲットデバイスを 1024 台まで接続することができます。

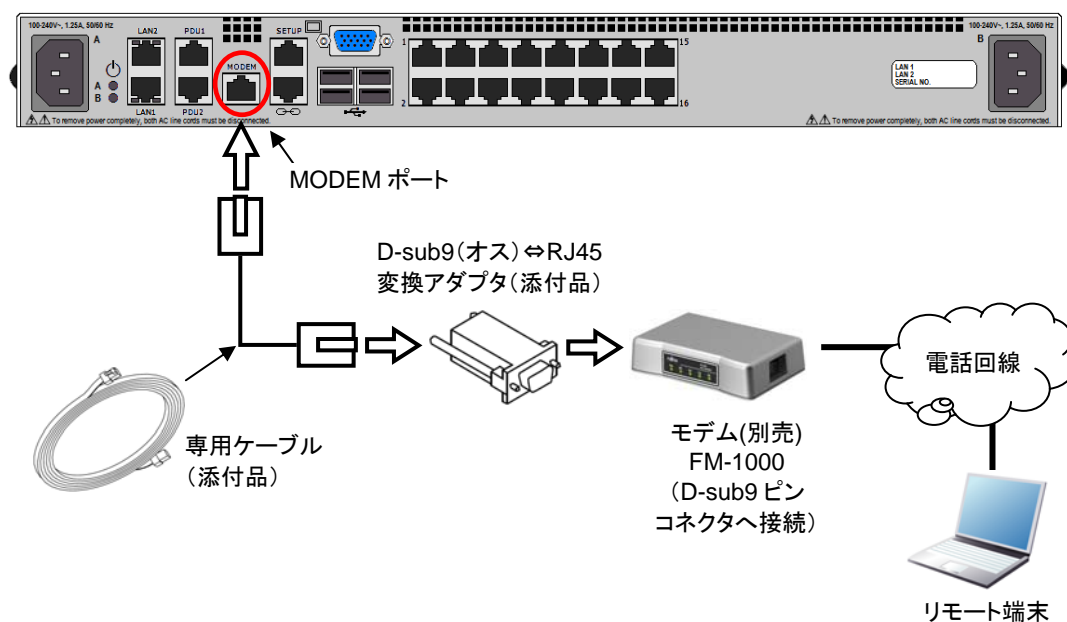
接続には、市販の Cat5e ストレートケーブルを用い、マスター装置側の任意のターゲットポートとスレーブ装置側のカスケードポートを接続します。

[マスター側装置]

操作方法の詳細については、下記をご参照ください。
📖 参照 3.19 カスケード接続 (112 ページ)

1.7.　モデム接続

イーサネット経由での本製品へのアクセスが利用できない場合の経路確保のために、V.34、V.90、V.92 のいずれかをサポートするモデム経由で本製品へアクセスすることができます。

本製品のモデム接続には、添付の専用ケーブルとD-sub9（オス）⇔RJ45 変換アダプタを用います。

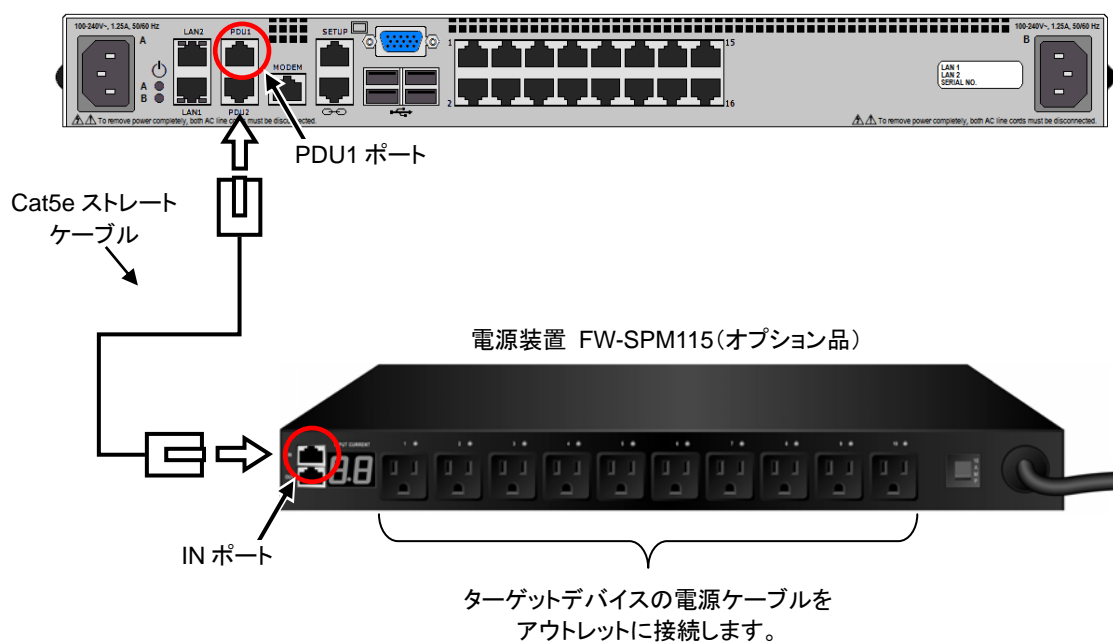
［FW-D2116NP の場合］

モデム接続に関する設定については、下記をご参照ください。

📖 参照 3.22 モデムの設定（126 ページ）

1.8. 電源装置との接続

本製品をオプションの電源装置と接続し、組み合わせてご利用いただくことにより、ターゲットデバイスの電源制御（ON/OFF 操作）を行うことができます。
本製品に電源装置は 2 台まで接続することができます（PDU1, PDU2 ポート）。

本製品の PDU1 あるいは PDU2 ポートと電源装置の IN ポートを電源装置に添付の Cat5e ストレートケーブルで接続します。

［FW-D2116NP の場合］

電源制御に関する設定については、下記をご参照ください。
📖 参照 3.20 電源装置の設定（114 ページ）

1.9. 接続に必要なもの

本製品をご利用になる上で添付品以外に必要なものを下に示します。

1) サーバーユニット

本装置とターゲットサーバーを接続するために用います。
📖 参照 1.4 サーバーユニット（8 ページ）

2) Cat5e ストレートケーブル

本装置とサーバーユニットの接続、本装置のネットワーク接続、本装置のカスケード接続などに用いる市販のケーブルです。

3) リモート操作端末は下記条件を満たすことが基本となります。

- ☐ 232c 接続用 D-Sub9 コネクタまたは相当がある
- ☐ 有線 Ethernet または無線 LAN 接続できる
- ☐ JRE 1.6 以降または相当が動作している
- ☐ web ブラウザで javascript が有効になっている、または有効にできる

重要（制限事項など）

① (共通) Java Runtime Environment (JRE)について

本製品をご利用頂くには JRE1.6 以降または相当が必要です。 ただしセキュリティ面から JRE1.7 update21 以降を推奨いたします (2013 年 5 月現在)。
また遠隔操作時に日本語入力環境を利用する場合は 32bit 版 JRE のみサポートします。英語入力を使うなどの場合には 64bit 版 JRE も許容します。

② (Windows) Internet Explorer について

64bit 版 Windows における Internet Explorer は、OS 標準で用意されているアイコン(スタートメニュー、タスクバーのクイック起動、デスクトップアイコンなど) からは 32bit 版が起動される仕組みとなっております(Windows Server 2003 ～ Windows Server 2012)。
64bit 版 Internet Explorer をご利用の際は 64bit 版の EXE を直接起動するか、そのショートカットを作成するなどして利用して下さい。 詳しくは Microsoft にお問い合わせ下さい。

③ (Windows) Javascript について

Windows Server 2008 R2 以降では Internet Explorer においてデフォルトで javascript が禁止されておりますが、本製品をご利用頂くには javascript が必要です。Internet Explorer のセキュリティ設定を調整して頂くか、FireFox 等他のブラウザの利用も検討してください。

④ (共通) 既知の問題について

本製品のビュワープログラム(java アプレット)は 64bit の JRE に対応しておらず、日本語入力出来ないなどの不具合があります。 この問題はファームウェアの改訂で解決する予定ですが、解決されるまでは 32bit 版 JRE をご利用下さい。 32bit 版と 64bit 版を併用する場合、可能でしたら 32bit→64bit 版の順にインストールしてください。 その後、拡張子 jnlp ファイルへの関連づけを 32bit 版 JRE に変更することで対処出来ます。

Windows の例) ¥Program Files(x86)¥Java¥jre7¥bin¥javaws.exe

Firefox などの IE 以外のブラウザをご利用頂くと、32bit 環境と 64bit 環境の正しい組合せを選択実行することができますので、そちらもご検討下さい。
java の環境設定はその他の java 関連の動作環境との調整が必要ですので、上記の対策が出来ない場合には、統合管理ソフトウェア DSView の導入もご検討下さい。DSView 環境では端末毎にビューアをローカルインストールする為、Java の制限事項に左右されません(Windows 専用)。

⑤ (共通) 動作確認済み OS (2013 年 5 月現在)

Windows : XP SP3 以降, Vista SP1 以降, 7 SP1 以降, Windows 8
Windows Server : 2003 R2, 2003 R2 x64, 2008, 2008 R2, 2012

Linux 系について

本製品で起動される "セッションビューア" は java の動作環境に左右されます。また、リモート側端末の入力ロケール(国、言語)設定およびキーボードドライバと、ターゲット側の入力ロケールとキーボードドライバとの設定・機能マッチングに大きく左右されます。
ディストリビューション毎の対応内容については本書の対象外とさせて頂きます。

その他の OS について

ブラウザ経由の OBWI 操作に支障はありません。
java アプレットをネイティブで動作させられない環境はサポート外となります。

4) スイッチングハブなど

本装置のネットワーク接続のためのルーター、スイッチングハブなどです。

5) ローカル接続用キーボード、マウス、モニター

ローカルユーザーインターフェースから操作するためのキーボード、マウス、モニターです。キーボード および マウスは USB コネクタで接続するタイプをご用意ください。

下記はご利用の環境構成に応じて必要なものになります

6) シリアルコンソール端末

本装置の SETUP ポートからのコンソールアクセスを行う場合、RS-232C インターフェース（D-sub9pin）を持つ PC が必要です。ハイパーターミナルなどのターミナルソフトがインストールされている必要があります。
📖 参照 Chapter 5 - シリアルコンソール（223 ページ）

7) モデム

電話回線によるアクセス経路を構成する場合、モデムが必要です。
📖 参照 1.7 モデム接続（13 ページ）

8) 電源装置（オプション品）

ターゲットデバイスの電源制御を合わせて行う場合、別売りの電源装置が必要です。
購入先にお問い合わせください。
📖 参照 1.8 電源装置との接続（14 ページ）

Chapter 2 - 基本操作

本製品を使用して、遠隔地からネットワーク経由でターゲットデバイスを操作するための基本的な操作手順について説明しています。

本章の内容

2.1.　基本操作の流れ

本製品を使用し、ネットワーク経由でターゲットデバイスを操作する基本的な手順について、以下に示します。

Step1　本装置を接続する
本装置をターゲットデバイス、ネットワークなどと接続し、リモート操作の準備を行います。
参照　2.2 本装置の接続（19 ページ）

↓

Step2　本装置の IP アドレスを設定する
本装置にローカルキーボード、マウス、モニターを接続し、IP アドレスを設定します。
参照　2.3 IP アドレスの設定（初期導入時）（21 ページ）

↓

Step3　リモート端末から本製品にアクセスする
ネットワーク上のリモート端末から本製品にアクセスし、OBWI から「ユーザー名」、「パスワード」を入力してログインします。
参照　2.4 リモート端末からのアクセス（25 ページ）

↓

Step4　ビデオセッションビューアを起動する
ビデオセッションビューアを起動し、ターゲットデバイスの操作を開始します。
参照　2.5 ビデオセッションビューアの起動（28 ページ）

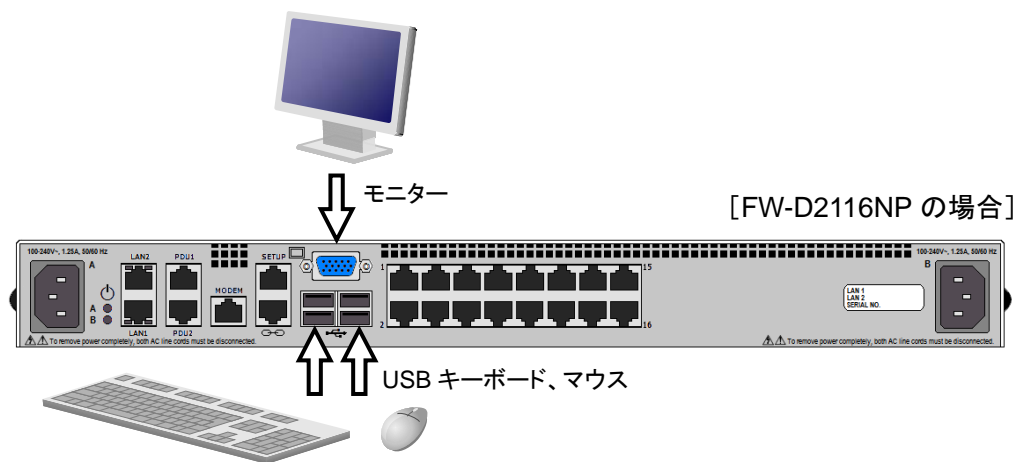
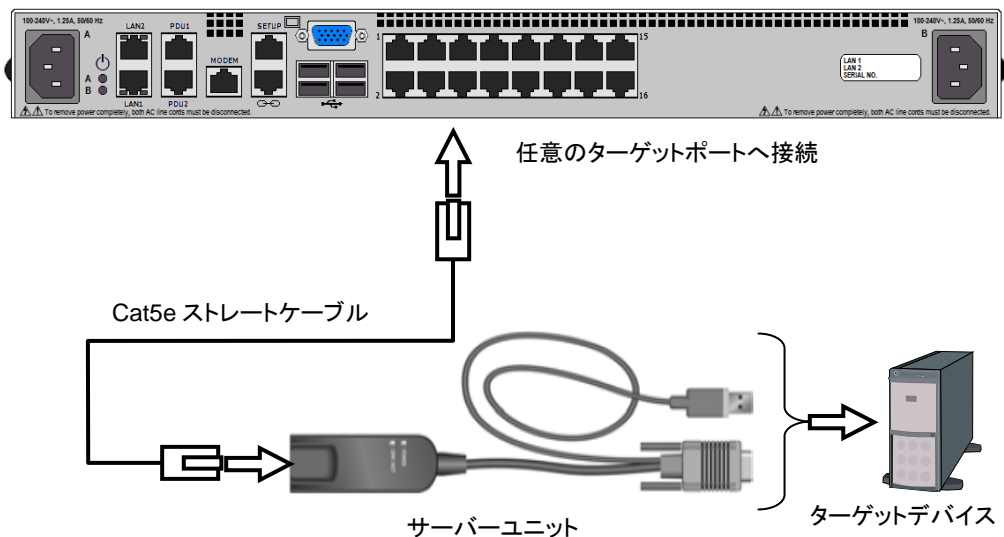
↓

Step5　ターゲットデバイスを操作する
ビデオセッションビューアの操作画面からターゲットデバイスを操作します。
参照　2.6 ターゲットデバイスの操作（32 ページ）

↓

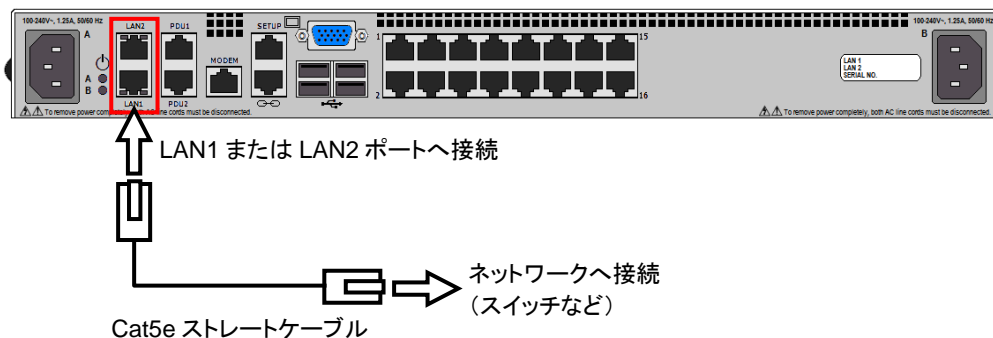
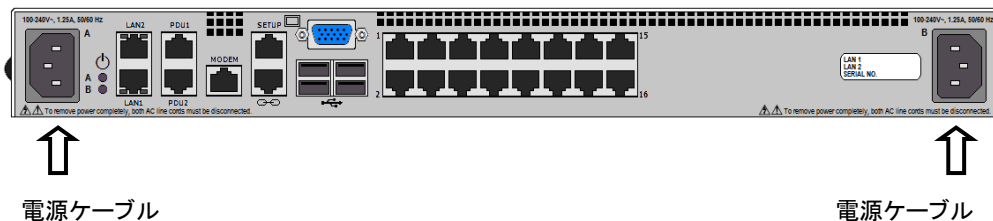
Step6　操作を終了し、ログアウトする
ビデオセッションビューアを終了し、OBWI からログアウトします。
参照　2.7 操作の終了、ログアウト（36 ページ）

2.2. 本装置の接続

製品本体のローカルポート、ターゲットポート、ネットワークポートへの接続を行い、電源を投入します。
ローカル操作用の接続を行います。製品背面の D-Sub 15pin(DE15) コネクタ、USBコネクタにモニター、キーボード、マウスを接続します。

サーバーユニット および 市販の Cat5e ストレートケーブルを用いて、製品本体とターゲットデバイスの接続を行います。接続するターゲットデバイスの数だけ同様に接続を行います。

重要

本製品は初期状態で **サーバーユニットの自動アップグレードが有効** になっております。アップグレード時間はサーバーユニット毎に約 7 分かかりますが、その間、**本体側の電源を切らないようお願い致します。**自動アップグレードの対象は DSM02 シリーズのサーバユニットとなります。本製品に取り付けの際は予めご了承ください。

参照 3.18.3 サーバーユニットのアップグレード（109 ページ）

本装置の LAN1 もしくは LAN2 コネクタに市販の Cat5e ストレートケーブルを用いて、ネットワークスイッチなどと接続します。

本製品に添付の電源ケーブル 2 本を接続し、製品本体の電源を投入します。添付品以外の電源ケーブルを使用しないでください。

本装置は電源ケーブル 1 本でも動作しますが、2 本ご使用いただいて冗長動作させることもできます。

重要

本製品は初期状態で **サーバーユニットの自動アップグレードが有効** になっております。アップグレード時間はサーバーユニット毎に約 7 分かかりますが、その間、**本体側の電源を切らないようお願い致します。**自動アップグレードの対象は DSM02 シリーズのサーバユニットとなります。本製品に取り付けの際は予めご了承ください。

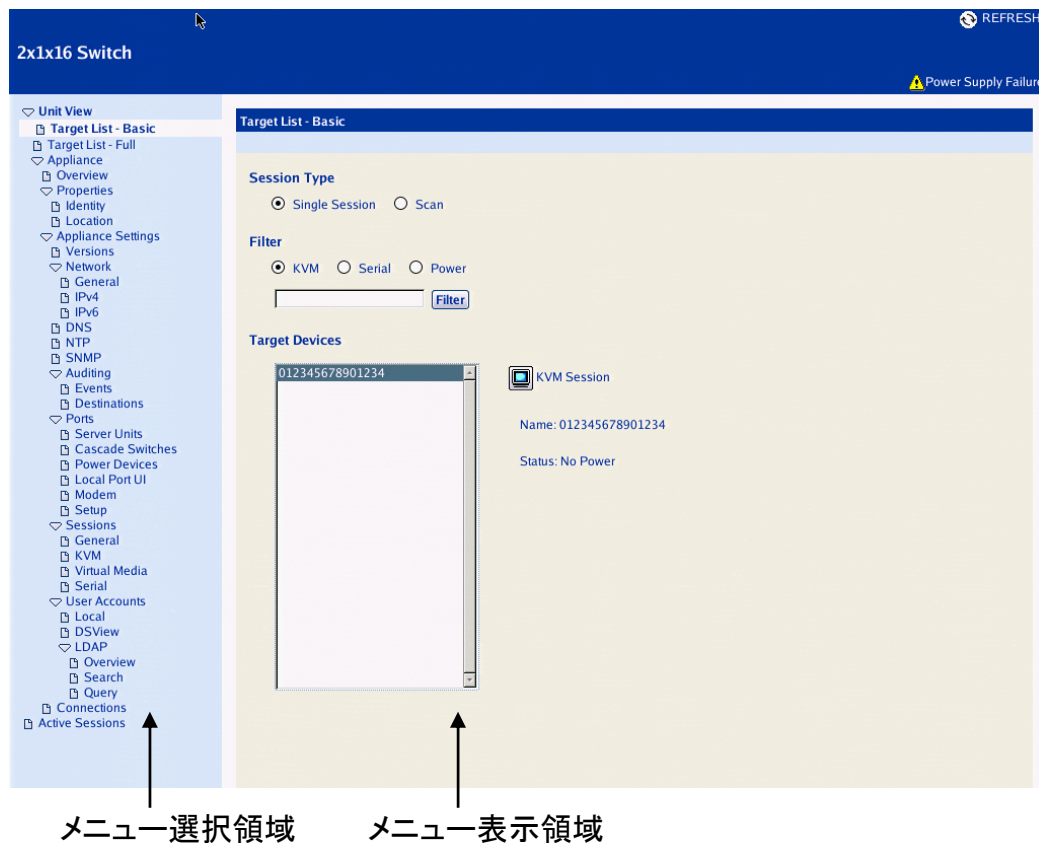
参照 3.18.3 サーバーユニットのアップグレード（109 ページ）

2.3. IP アドレスの設定（初期導入時）

本装置の初期設定として、IP アドレスの設定をローカルポートに接続したキーボード、マウス、モニターによる、ローカルポート ユーザーインターフェース（以降、ローカル UI と省略します。）から行います。

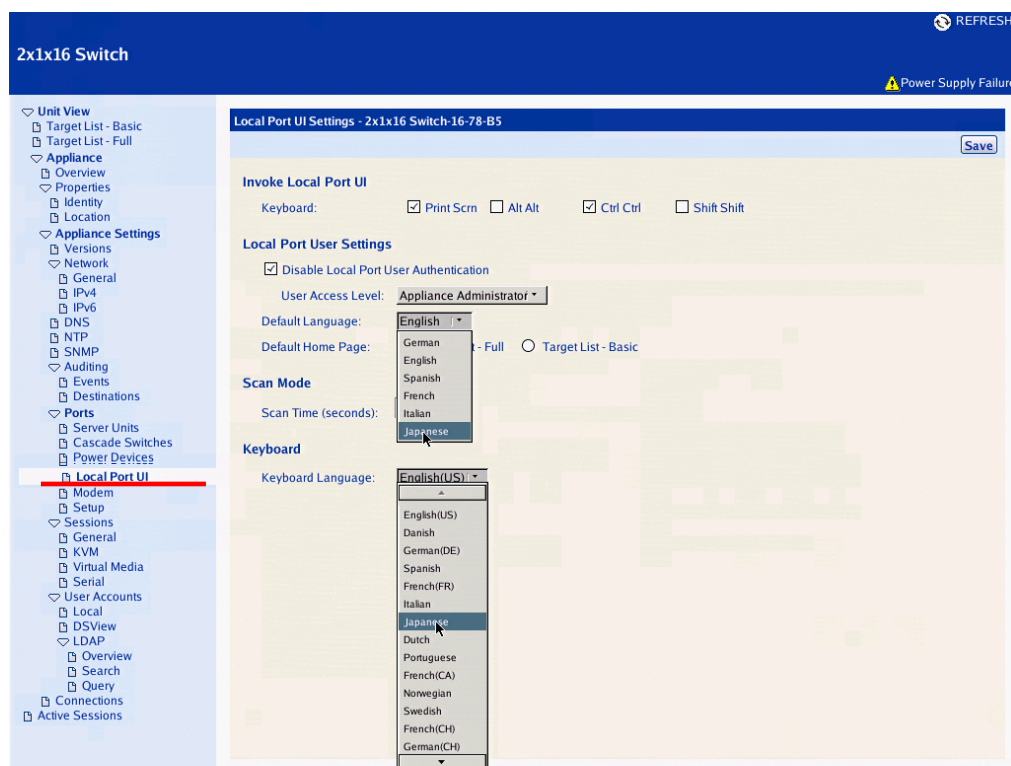
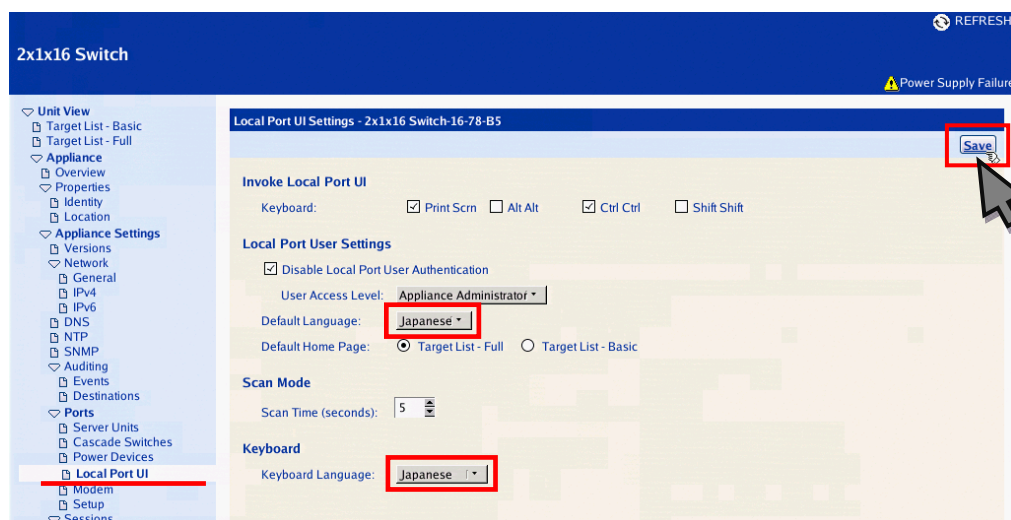
ローカルキーボード、マウス、モニターの接続については、下記をご参照ください。
参照 2.2 本装置の接続 （19 ページ）

2.3.1 ネットワークの設定

デフォルト設定状態で本装置が起動すると、ローカルモニターには、下のような画面が表示されます。ローカルポート UI の初期設定は、英語表示です。

画面左側のメニュー選択領域において、階層表示されている各種メニューから任意の項目を選択してクリックすると画面右側のメニュー表示領域にその内容が表示されます。

重要

ローカルポート UI と OBWI との違いは 125 ページ **重要：ローカルポートと OBWI の違い**を参照してください。

ローカルポート UI を日本語表示に変更するには、画面左のメニュー選択領域において、「Unit View」-「Appliance」-「Appliance Settings」-「Ports」に属する「Local Port UI」をクリックすると「Local Port UI Settings」ページが表示されます。

Default Language を Japanese に、Keyboard Language を Japanese にしてから［Save］ボタンをクリックします。

その後、画面右上の REFRESH を行うか、異なるメニューを表示すると日本語に切り替わります。

重要

ローカルポート UI と OBWI との違いは 125 ページ **重要：ローカルポートと OBWI の違い**を参照してください。

2.3.2　ネットワークの設定

ローカルポート UI から本装置のネットワーク設定を行います。
ここでは、下に示す スタティックな IPv4 アドレスを設定する場合の例を示します。

IP アドレス	:	192.168.1.100
サブネットマスク	:	255.255.255.0
デフォルトゲートウェイ	:	192.168.1.1

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ネットワーク」-「IPv4」をクリックすると「アプライアンス IPv4 設定」ページが表示されます。

"IPv4 を有効にする" にチェックを入れ、アドレス、サブネット、ゲートウェイの各項目に値を入力し、右上の[保存]ボタンをクリックします。

以上で、ネットワーク設定は完了です。すぐに設定は反映されます。

重要

ローカルポート UI と OBWI との違いは 125 ページ **重要：ローカルポートと OBWI の違い**を参照してください。

2.4. リモート端末からのアクセス

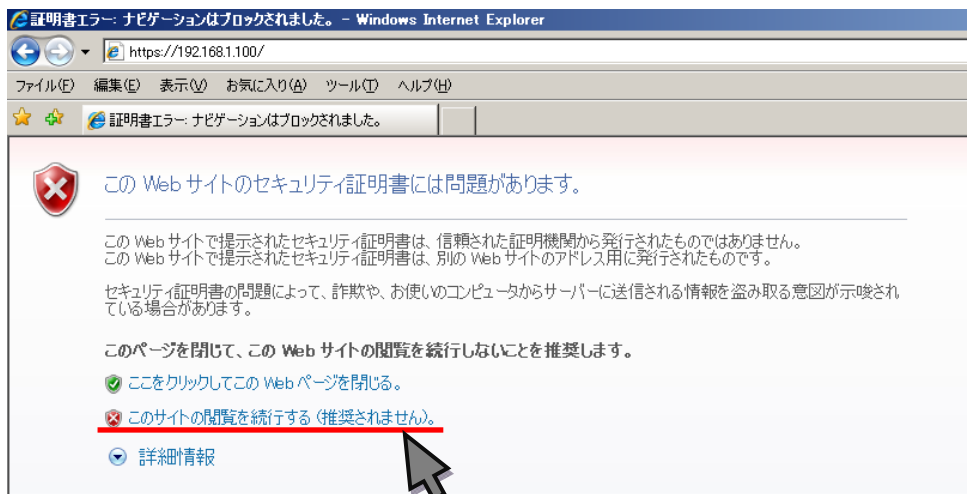
ネットワーク上のリモート端末から本装置の操作を行う場合、ブラウザを用いた Web ユーザ・インターフェース（以降、OBWI と省略します。）から実行します。

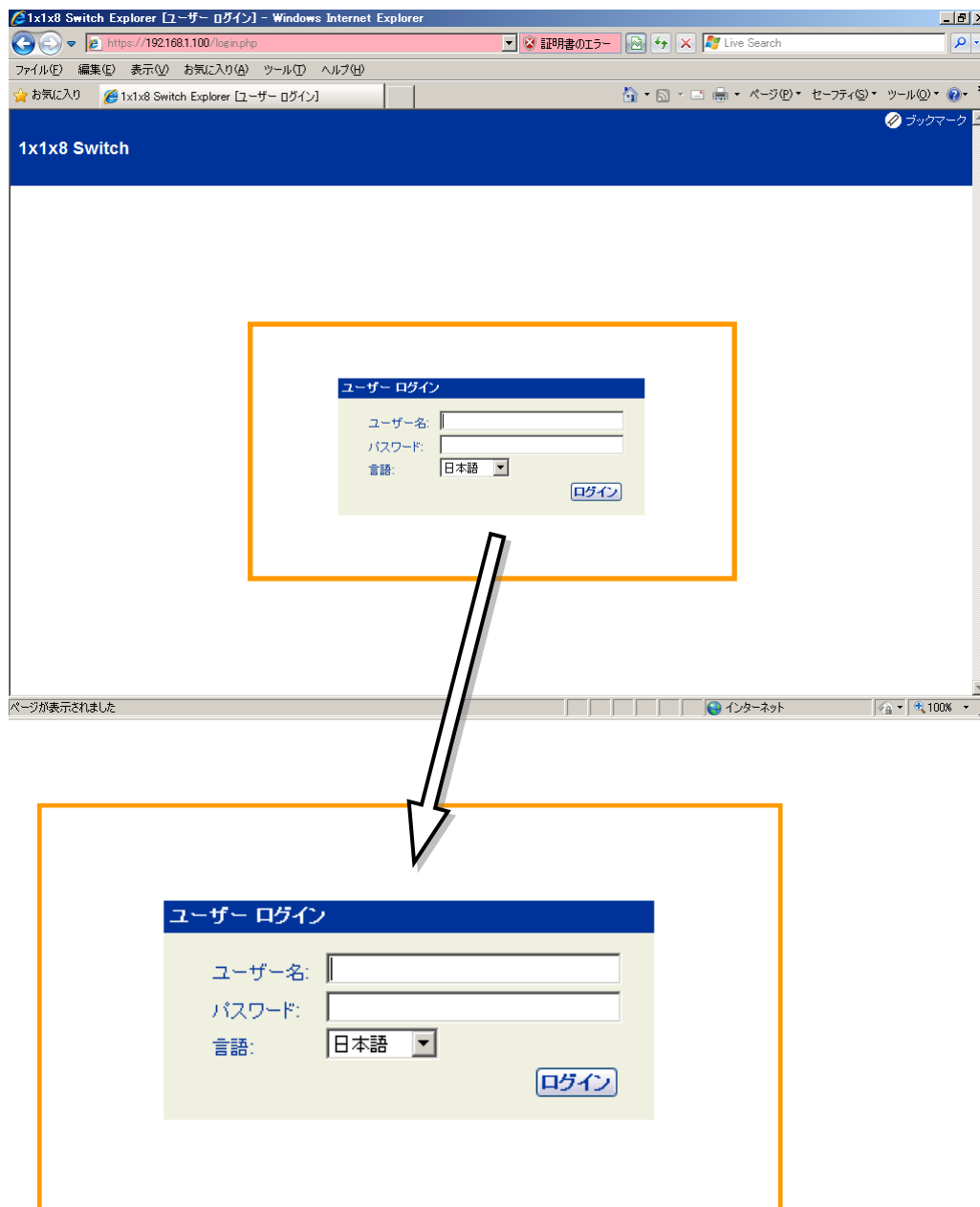
ネットワーク上のリモート端末から本装置の OBWI にログインする手順について説明します。

リモート端末でブラウザを起動し、設定した IP アドレスに対して https プロトコルでアクセスします。（本書では、Microsoft Internet Explorer を用いてアクセスする例を示します。）
IP アドレスは、以下のように設定されているとします。

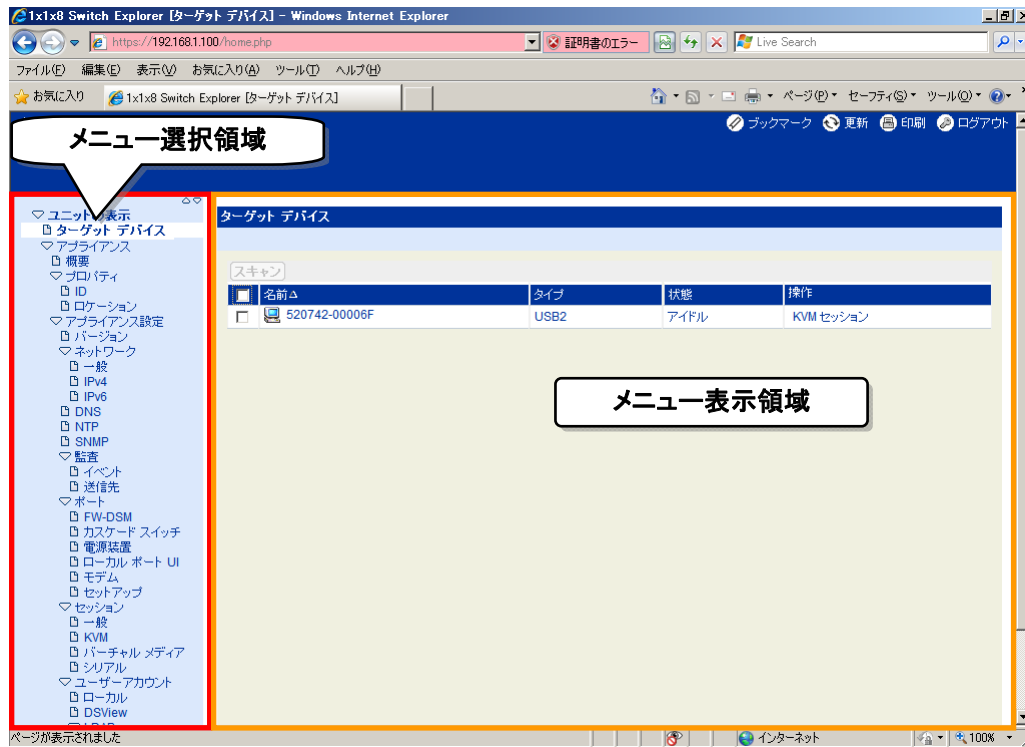
➢ IP Address: 192.168.1.100

セキュリティ証明書に関するメッセージが表示されます。”このサイトの閲覧を続行する” をクリックしてください。

2

基本操作

Web ページのログイン画面が表示されます。デフォルトで管理用アカウント: admin および そのパスワード: admin が設定されています。ユーザー名: admin, パスワード: admin を入力し、[ログイン]ボタンをクリックしてください。

セキュリティ確保のため、admin ユーザーのパスワード変更をお勧めします。

📖 参照 3.29.2 ユーザー設定の変更（138 ページ）

ログインすると、下のようなページが表示されます。画面左のメニュー選択領域において、階層表示されているメニューから任意の項目を選択してクリックすると右の表示領域にその内容が表示されます。
ログイン直後は､「ターゲットデバイス」ページが表示され、現在本装置に接続されている、あるいは、以前接続されたことがあるサーバーユニットがリスト表示され、状態を確認することができます。

本装置の設定については、全てこの OBWI 上で行うことができます。詳細については、下記をご参照ください。

参照 Chapter 4 - ビデオセッション（167 ページ）

2.5. ビデオセッションビューアの起動

リモート端末から OBWI によって、本装置にログインした後、ターゲットデバイスを操作するには、ビデオセッションビューアという操作画面を起動します。
ビデオセッションビューアを使用するためには、あらかじめリモート端末に Java Runtime Envoronment (JRE)インストールしておく必要があります。

OBWI にログインすると、下のように現在接続されている、あるいは、以前接続されたことがあるサーバーユニットがリスト表示されます。サーバーユニットに設定された名称、サーバーユニットのタイプ、現在の状態（使用中／アイドル）が確認できます。ターゲットデバイスを操作する場合は、”KVM セッション” をクリックします。

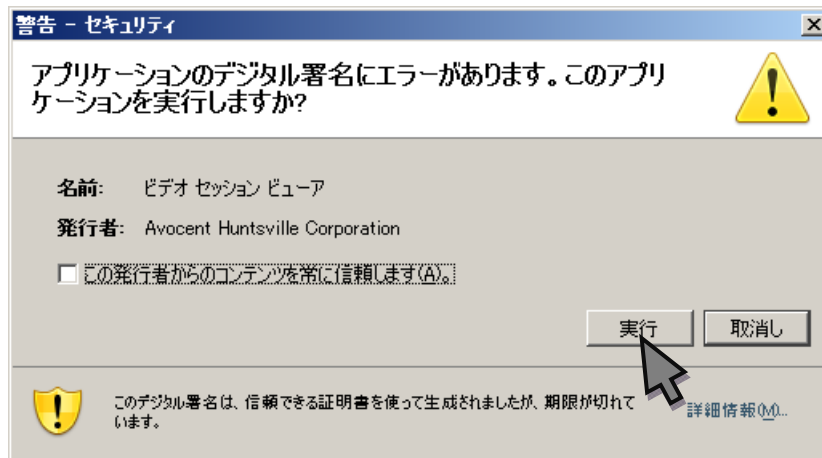
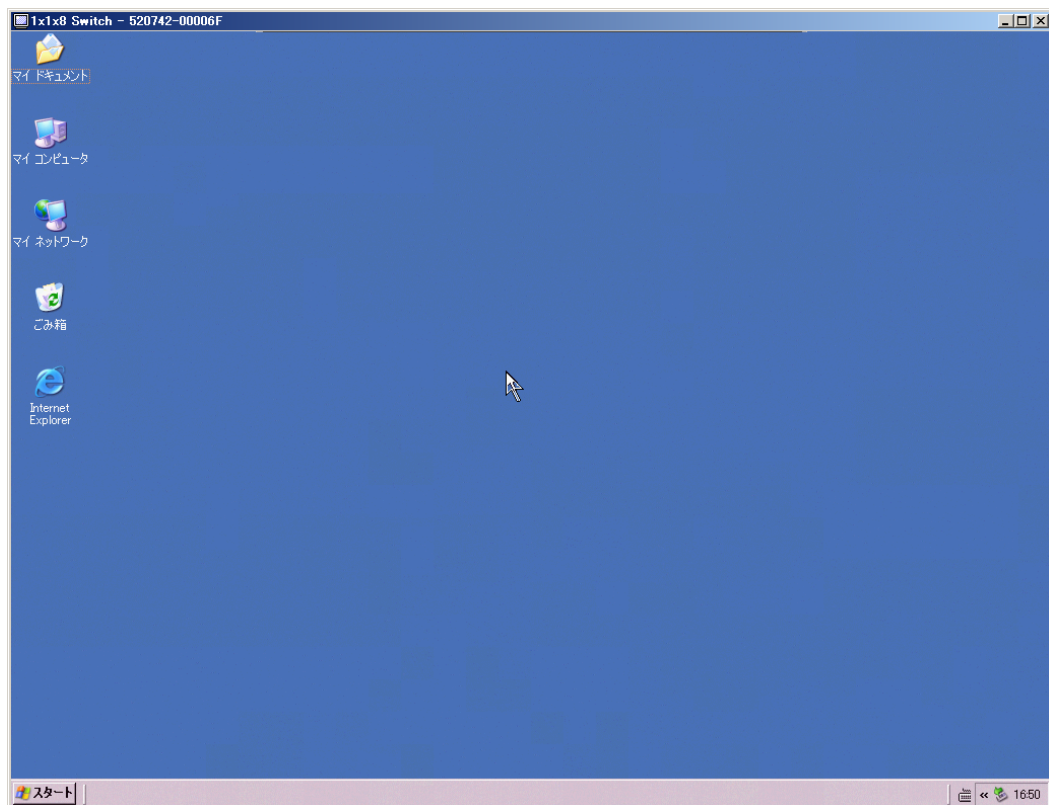
名前項目に表示されるインジケーター表示により、以下の状態を示します。

表示	状態	説明
	アイドル	ターゲットデバイスは電源が入っており、アクセス可能な状態です。
	使用中	ユーザーがターゲットデバイスにアクセスしている状態です。
	電源なし	ターゲットデバイスは電源オフ状態、あるいは、本装置とサーバーユニットが接続されていない状態です。
	アップグレード中	サーバーユニットのアップグレード中です。 ターゲットデバイスへのアクセスはできません。

重要（アップグレード中 について）

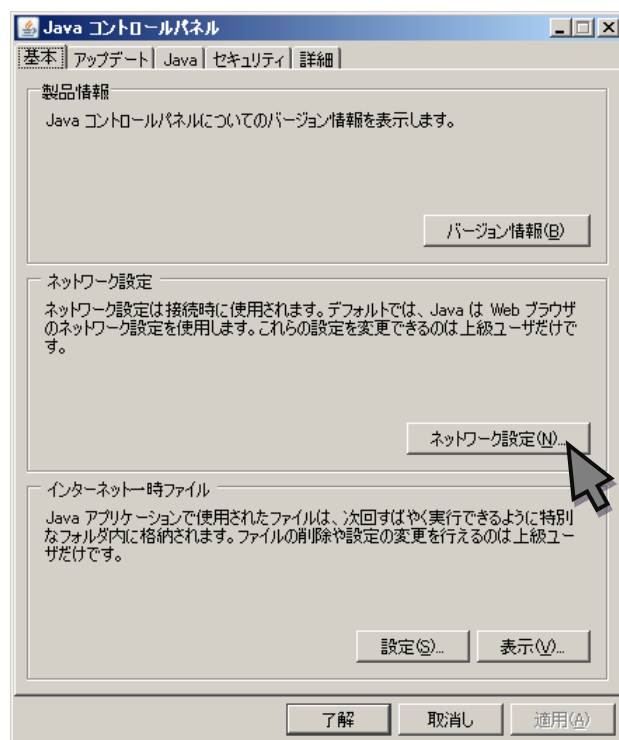
本製品は初期状態で **サーバーユニットの自動アップグレードが有効** になっております。アップグレード時間はサーバーユニット毎に約 7 分かかりますが、その間、**本体側の電源を切らないようお願い致します**。自動アップグレードの対象は DSM02 シリーズのサーバユニットとなります。本製品に取り付けの際は予めご了承ください。

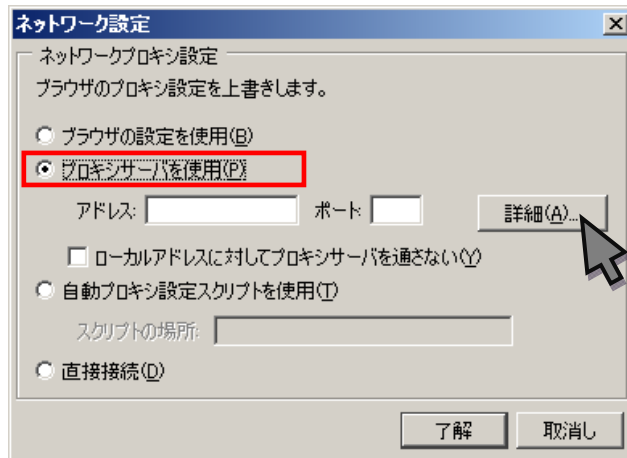
参照 3.18.3 サーバーユニットのアップグレード（109 ページ）

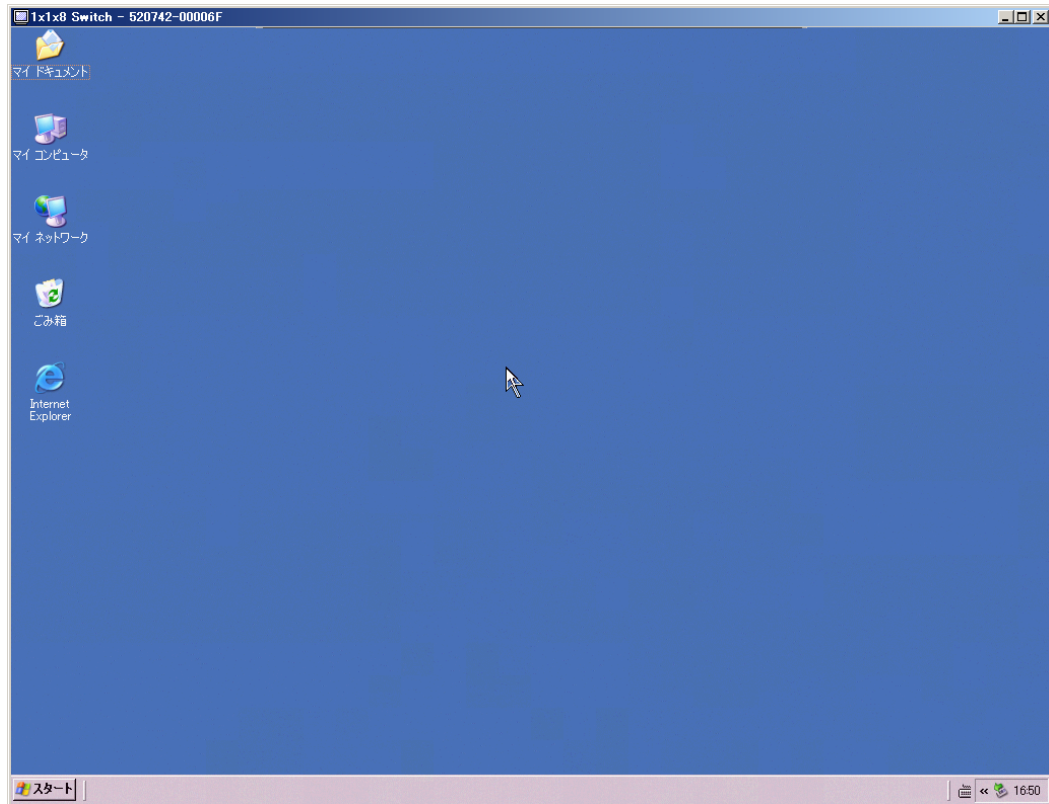
Java のアプリケーションが起動します。下のように警告メッセージが表示される場合は、「実行」ボタンをクリックします。

下のようなビデオセッションビューア画面が表示され、ターゲットデバイスの操作が可能となります。

重要

下のようなエラーメッセージが表示され、ビデオセッションビューア画面が表示されない場合は、下記の設定をご確認ください。

［Java 設定の確認］

コントロールパネルから「Java」を開き、下のようなウィンドウにおいて、「ネットワーク設定」ボタンをクリックします。

下のような、ネットワークの設定画面が表示されます。”プロキシサーバを使用” ラジオボタンをクリックし、「詳細」ボタンをクリックして適切なプロキシ設定を行ってください。

ネットワーク設定
ネットワークプロキシ設定
ブラウザのプロキシ設定を上書きします。
ブラウザの設定を使用(B)
プロキシサーバを使用(P)
アドレス: ポート: 詳細(A)...
ローカルアドレスに対してプロキシサーバを通さない(Y)
自動プロキシ設定スクリプトを使用(T)
スクリプトの場所:
直接接続(D)
了解 取消し

2.6. ターゲットデバイスの操作

ビデオセッションビューアには、ターゲットデバイスのデスクトップ画面が表示されます。

通常、ビデオセッションビューアからターゲットデバイスを操作する場合、リモート端末側のマウスカーソルとターゲットデバイスのマウスカーソルの２種類が表示されている状態となります。マウスカーソルの動作としては、リモート端末側のカーソル移動にターゲットデバイス側のカーソルが追従する形になります。

・白色で一回り小さいカーソルが
・ターゲットデバイス側のマウスカーソル
・透明で大きい方のカーソルが
リモート端末側のマウスカーソル
（カーソル形状は設定変更可能）

ビデオセッションビューアの詳細内容については、以下の章をご参照ください。

📖 参照 Chapter 4 - ビデオセッションビューア（167 ページ）

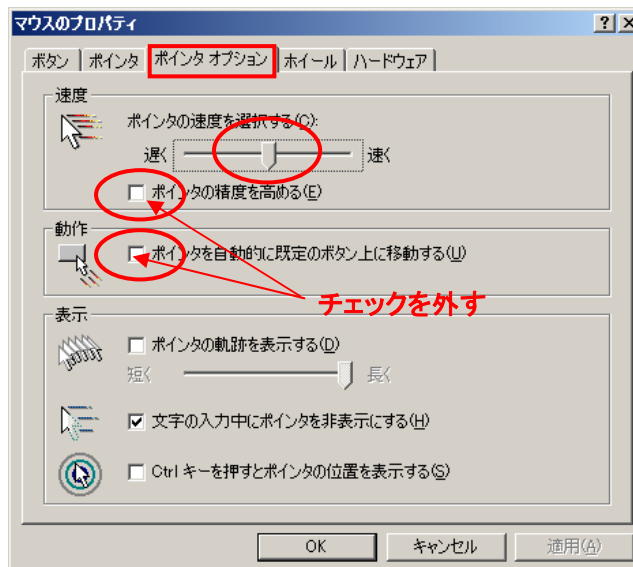
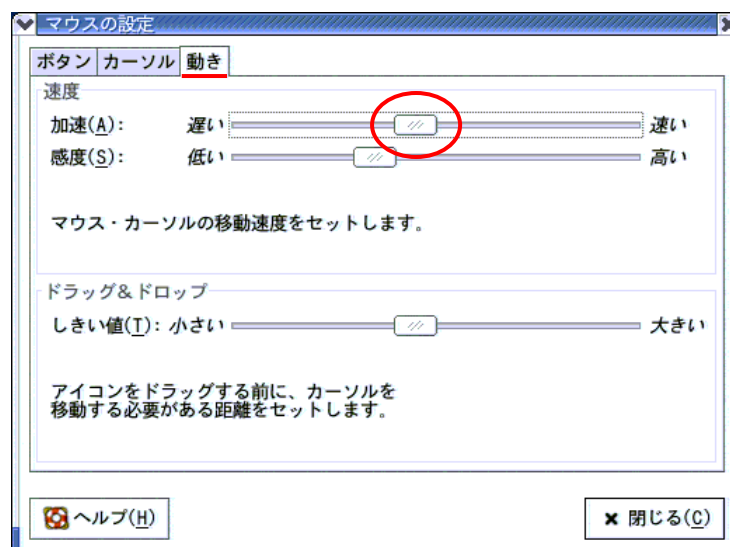
重要

リモート端末とターゲットデバイスのカーソル位置を一致させるため、ターゲットデバイスのマウスの加速度設定を無効にする必要があります。

📖 参照 2.6.1 ターゲットデバイスの初期設定（33 ページ）

2.6.1　ターゲットデバイスの初期設定

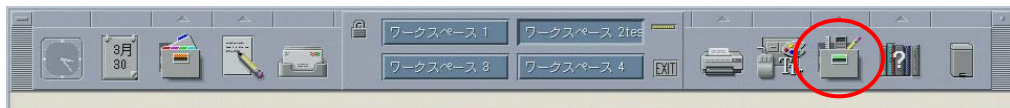
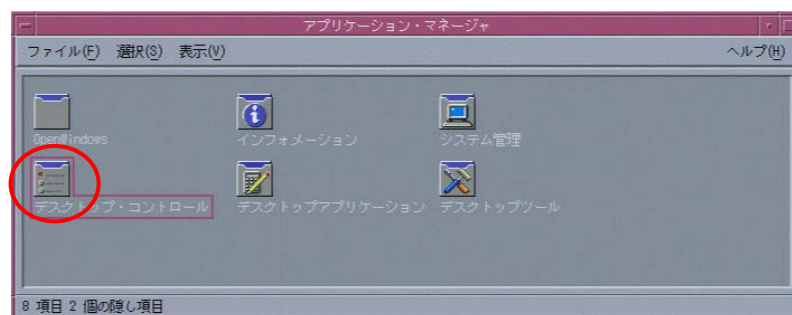
リモート端末とターゲットデバイスのマウスカーソルを一致させるには、以下のようにターゲットデバイスのマウスの設定を行い、「加速」設定を無効にする必要があります。

➢ ターゲットデバイスが Windows OS の場合
「コントロールパネル」の「マウス」をクリックし、マウスのプロパティを表示します。
Windows XP, Windows Server 2003, Windows 7 などの場合
→ **速度: 中**
→ **ポインタの精度を高める: チェックを外す**
→ **ポインタを自動的に規定のボタン上に移動する: チェックを外す**

➢ ターゲットデバイスが RedHat Linux（GNOME） の場合
「個人設定」ー「マウス」をクリックし、「マウスの設定」ダイアログを表示します。
→ **加速: 中（やや遅い側）** 確認しながら調整してください。

➢ ターゲットデバイスが Solaris（GNOME）の場合

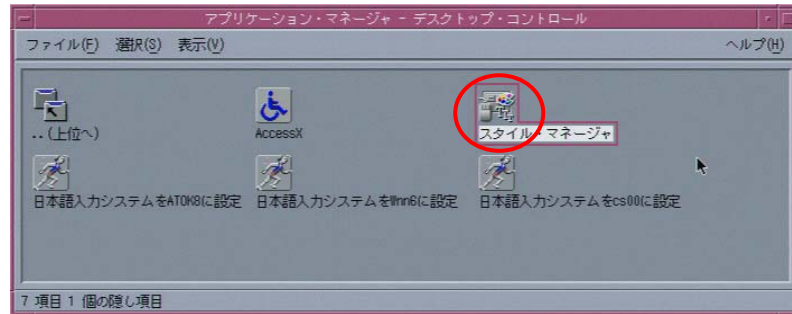
「起動メニュー」ー「設定」ー「デスクトップの設定」ー「マウス」をクリックし、「マウスの設定」ウィンドウを表示します。

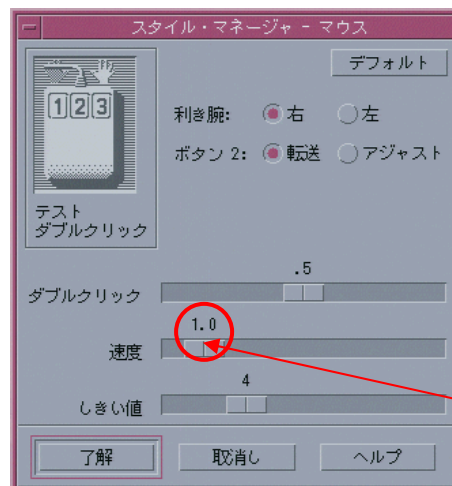
→ **加速: 中（やや低速側）** 確認しながら調整してください。

➢ ターゲットデバイスが Solaris（CDE） の場合

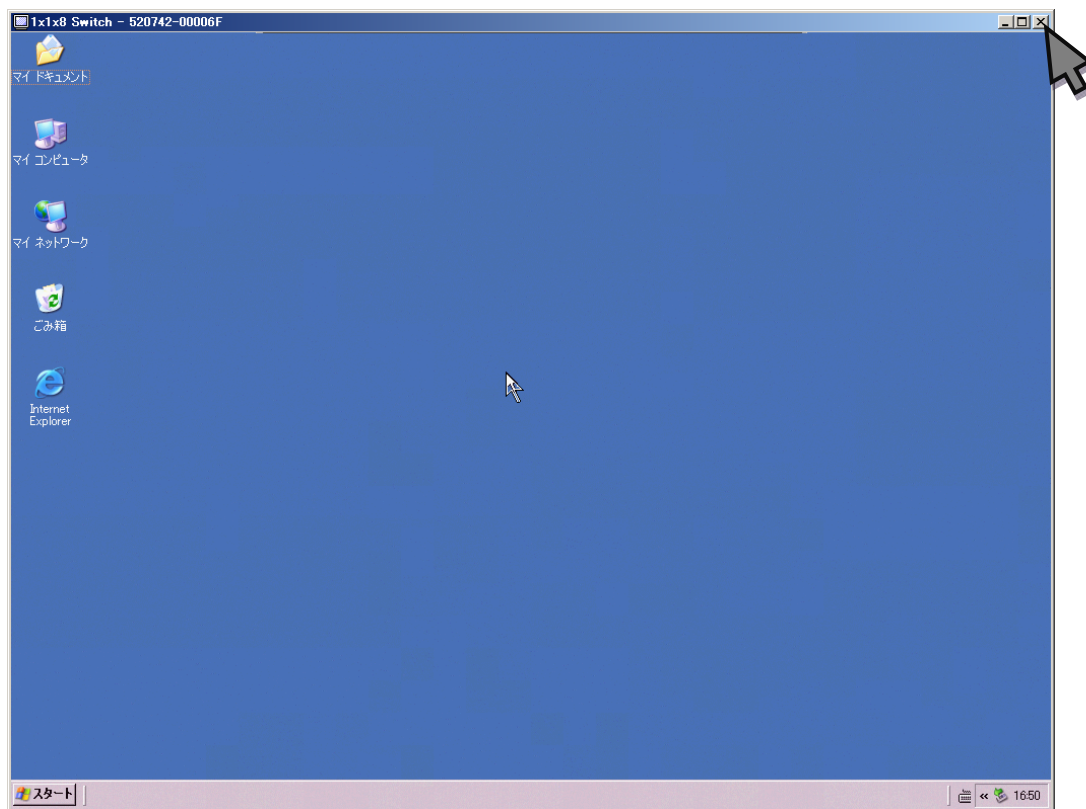
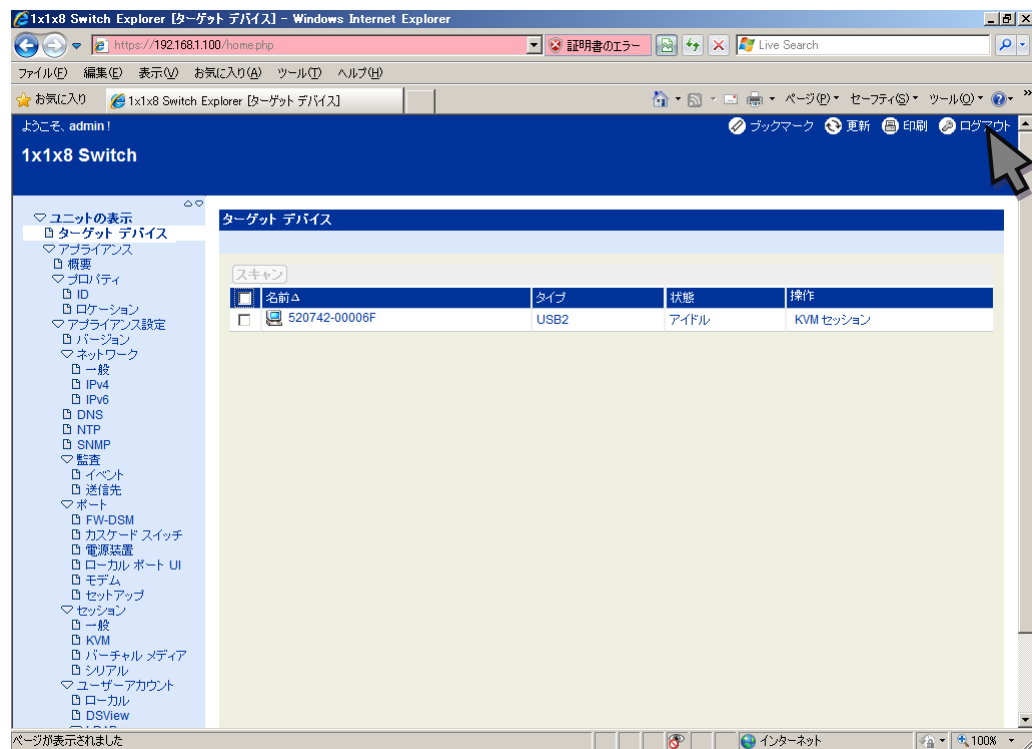
「ワークスペースメニュー」の「アプリケーション」アイコンをクリックします。

「アプリケーション・マネージャ」ウィンドウが開きます。「デスクトップ・コントロール」アイコンをダブルクリックします。

次のページへ続く ⇒

⇒ 前のページからの続き

「アプリケーション・マネージャ ー デスクトップ・コントロール」ウィンドウが開きます。「スタイル・マネージャ」アイコンをダブルクリックします。

「スタイル・マネージャ」ウィンドウが開きます。「マウス」アイコンをクリックします。

「スタイル・マネージャ ー マウス」ウィンドウが開きます。「速度」の値を 1.0 に設定し、「了解」ボタンをクリックします。

2.7. 操作の終了、ログアウト

ターゲットデバイスの操作が完了したら、ビデオセッションビューアを終了します。その後、OBWI をログアウトします。

ビデオセッションビューア画面の右上の[×]ボタンをクリックして、ビューア画面を閉じます。

OBWI の右上の ”ログアウト” をクリックします。ログアウトが実行され、再びログイン画面が表示されます。

以上で基本操作は終了です。機能詳細につきましては、次章からの説明をご参照ください。

Chapter 3 - ユーザーインターフェース

ネットワーク上のリモート端末からの On-board Web インターフェース(OBWI)、あるいは、ローカルのインターフェースから本装置の設定を行う方法について説明しています。

本章の内容

3.1.　ユーザーインターフェースの概要

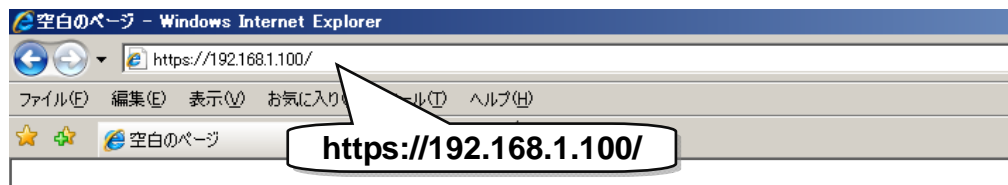
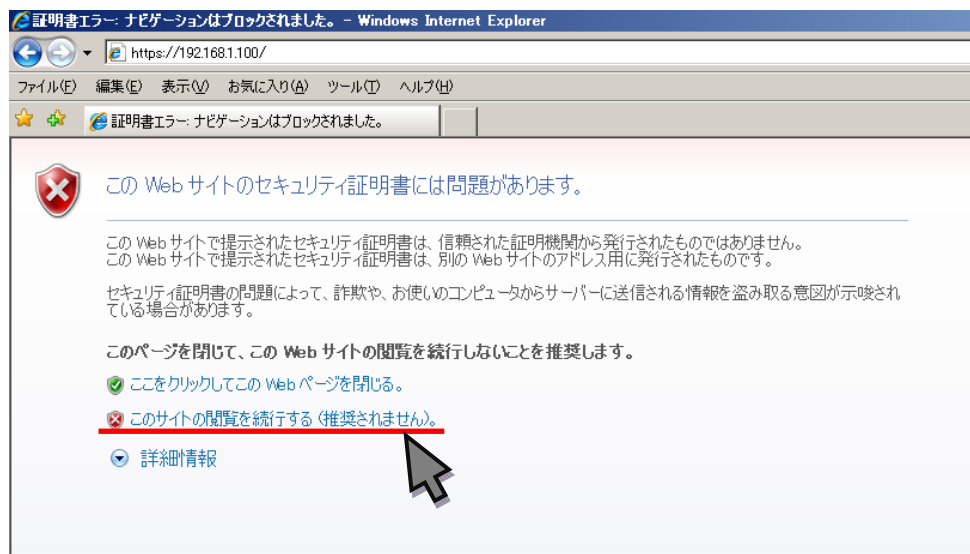
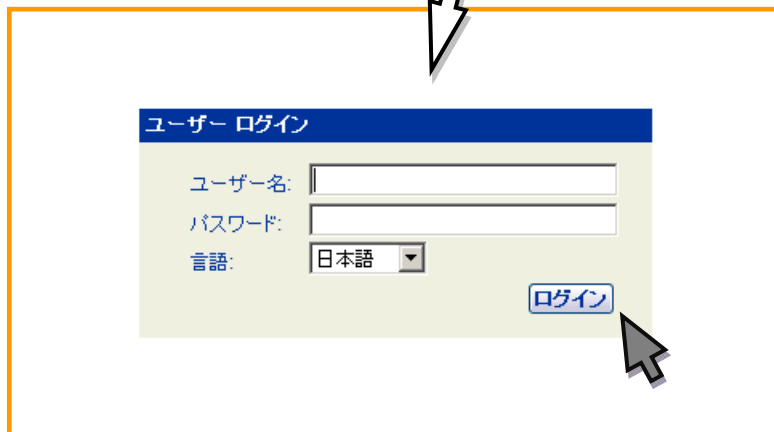
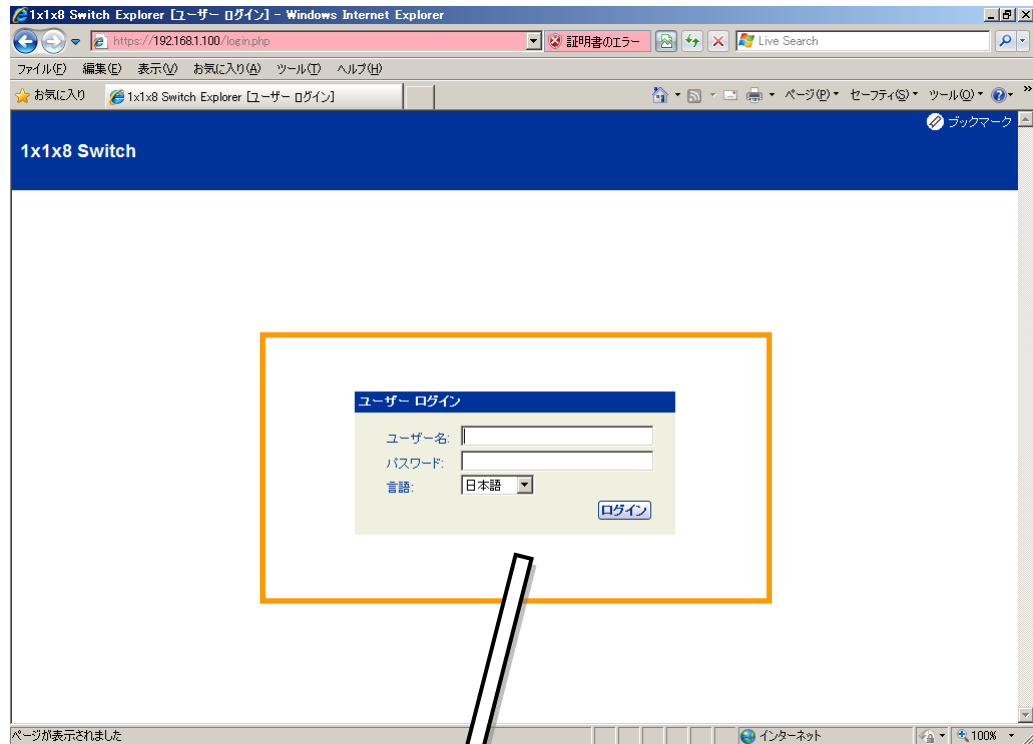
リモート端末からブラウザを用いて本装置の設定を行う、On-board Web インターフェース（OBWI）と本装置のローカルに接続したキーボード、マウス、モニターを用いて設定を行う、ローカルユーザーインターフェース（ローカル UI）の画面構成は同じものとなっています。

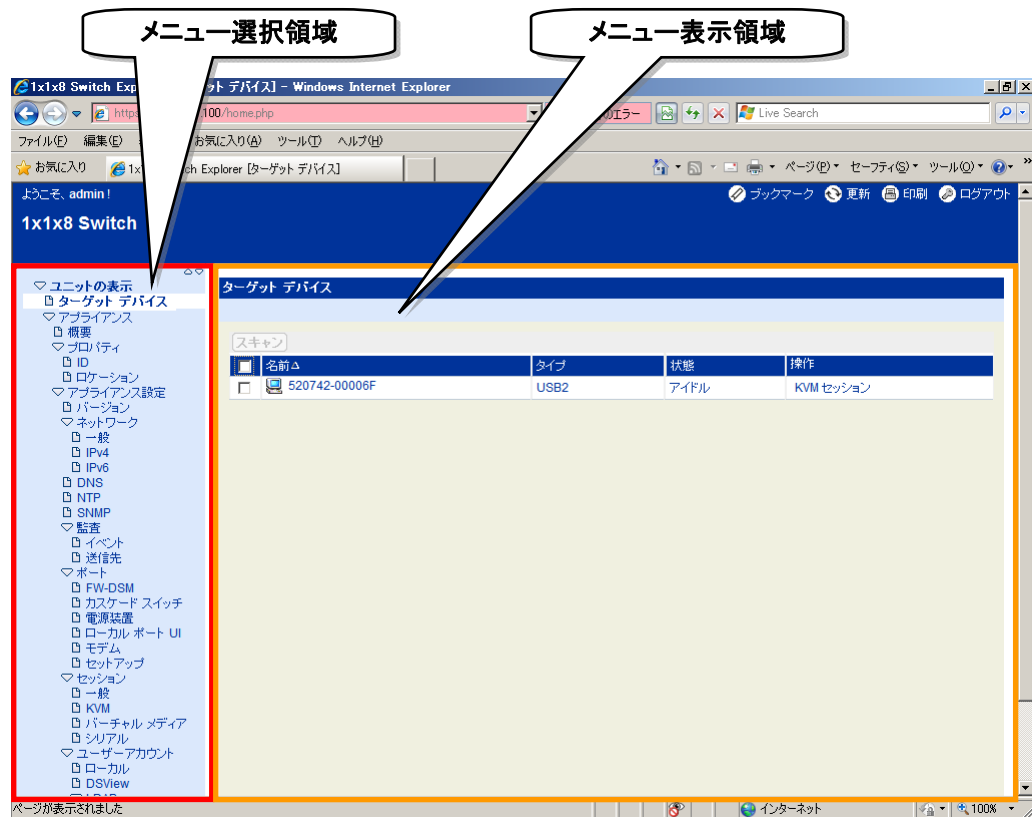
本章では、OBWI とローカル UI の操作画面について、ユーザーインターフェースとして、各設定・操作内容を説明します。

3.2.　ユーザーインターフェースへのログイン

ネットワーク上のリモート端末から OBWI を用いて、本装置にログインする手順を以下に説明します。

① リモート端末でブラウザを起動し、設定した IP アドレスに対して https プロトコルでアクセスします。（本書では、Microsoft Internet Explorer を用いてアクセスする例を示します。）IP アドレスは、以下のように設定されているとします。

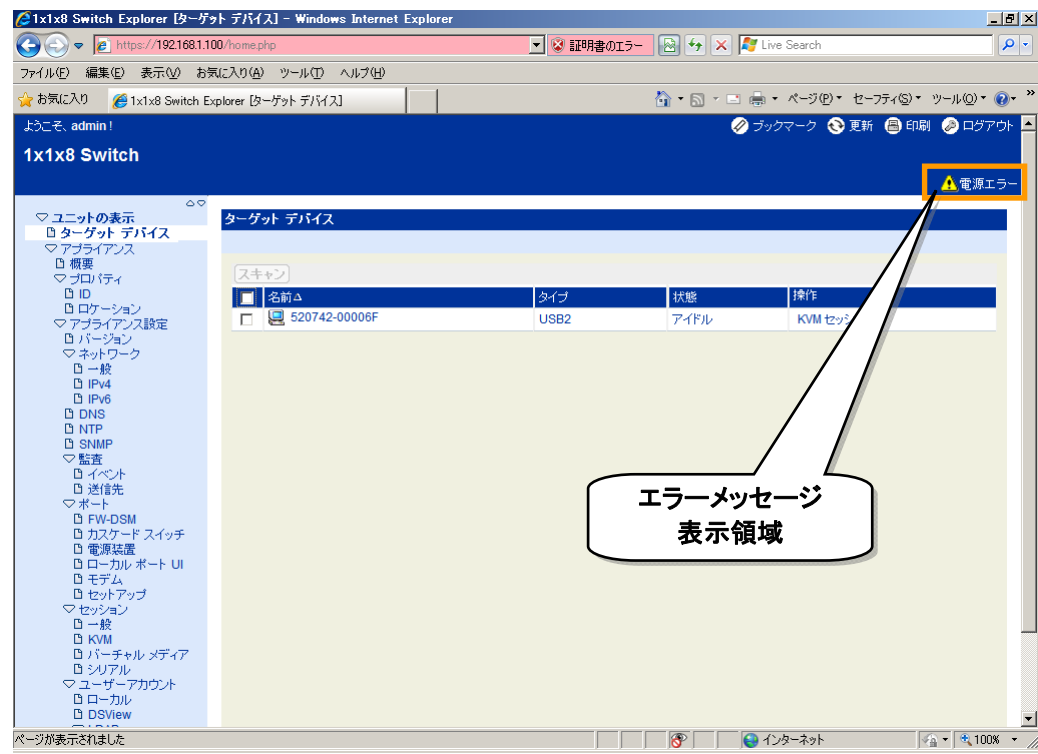
➢ IP Address: 192.168.1.100

② セキュリティ証明書に関するメッセージが表示されます。”このサイトの閲覧を続行する” をクリックしてください。

③ Web ページのログイン画面が表示されます。デフォルトで管理用アカウント: admin および パスワード: admin が設定されています。ユーザー名: admin, パスワード: admin を入力し、[ログイン]ボタンをクリックしてください。

セキュリティ確保のため、admin ユーザーのパスワード変更をお勧めします。

④ ログインすると、下のようなページが表示されます。画面左のメニュー選択領域において、階層表示されているメニューから任意の項目を選択してクリックすると右の表示領域にその内容が表示されます。
ログイン直後は、「ターゲットデバイス」ページが表示され、現在本装置に接続されているサーバーユニットの状態を確認することができます。

次項から、各操作および設定内容について説明します。

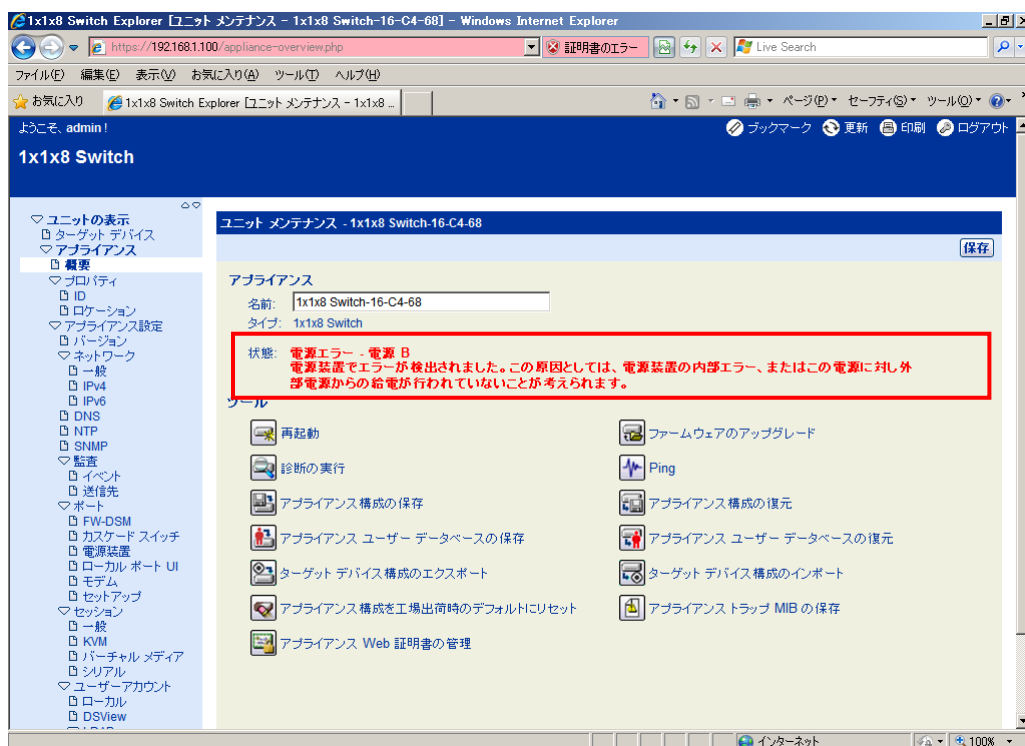
重要

社内イントラネットなどの構成において、プロキシサーバーを介して Web アクセスを行っているネットワーク環境では、OBWI 接続が不安定になる場合があります。
リモート端末上のブラウザ設定において、プロキシを使用しない設定（プロキシの例外設定に本装置の IP アドレスを追加する）にて OBWI 接続を行っていただけますようお願いいたします。

3.3. エラーメッセージの表示

装置本体において、ハードウェア的なエラーを検出するとユーザーインターフェース画面の右上にエラーメッセージが表示されます（下図参照）。

各表示内容によって、以下の状態を示します。

表示	説明
⚠電源エラー	電源装置でエラーが検出されました。この原因としては、電源装置の内部エラー、またはこの電源に対し外部電源からの給電が行われていないことが考えられます。
⚠ケース ファン エラー	内蔵の冷却ファンのうちの 1 台でエラーが検出されました。ユニットを点検してファンの通気口が塞がれていないことを確認してください。
⚠複数のアラート	上記の電源エラーおよびケースファンエラーが同時に検出されました。上記各項目について確認してください。

また、「ユニットメンテナンス」ページに下のような状態および確認事項が表示されます。
エラー発生時には、合わせてご確認ください。。

3.4. ターゲットデバイス操作の実行

OBWI からターゲットデバイスを操作する手順について説明します。

⑤ OBWI にログインすると、下のように現在接続されている、あるいは、以前接続されたことがあるサーバーユニットがリスト表示されます。サーバーユニットに設定された名称、サーバーユニットのタイプ、現在の状態（使用中／アイドル）が確認できます。ターゲットデバイスを操作する場合は、"KVM セッション" をクリックします。

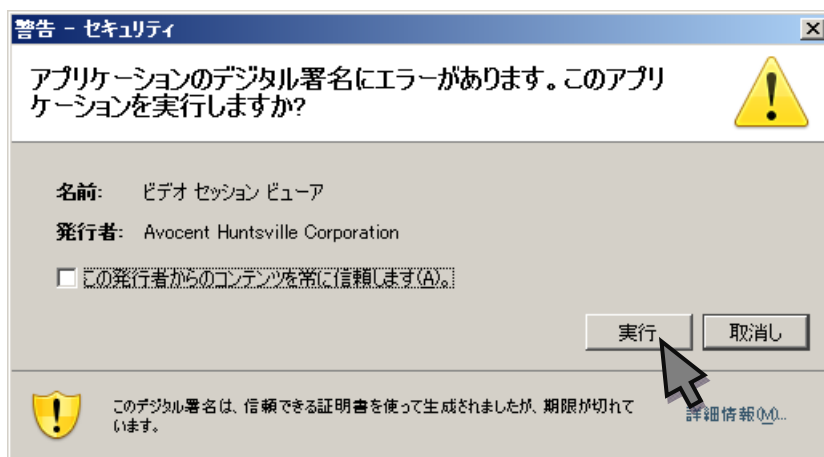
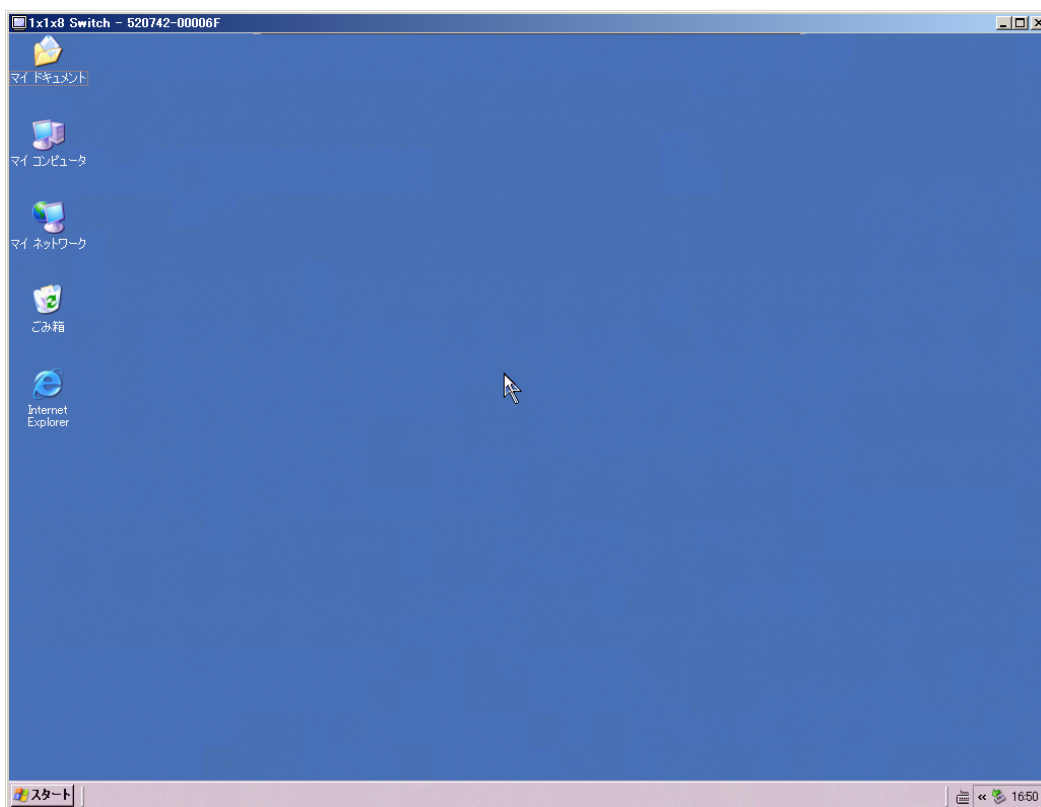
名前項目に表示されるインジケーター表示により、以下の状態を示します。

表示	状態	説明
	アイドル	ターゲットデバイスは電源が入っており、アクセス可能な状態です。
	使用中	ユーザーがターゲットデバイスにアクセスしている状態です。
	電源なし	ターゲットデバイスは電源オフ状態、あるいは、本装置とサーバーユニットが接続されていない状態です。
	アップグレード中	サーバーユニットのアップグレード中です。 ターゲットデバイスへのアクセスはできません。

重要（アップグレード中 について）

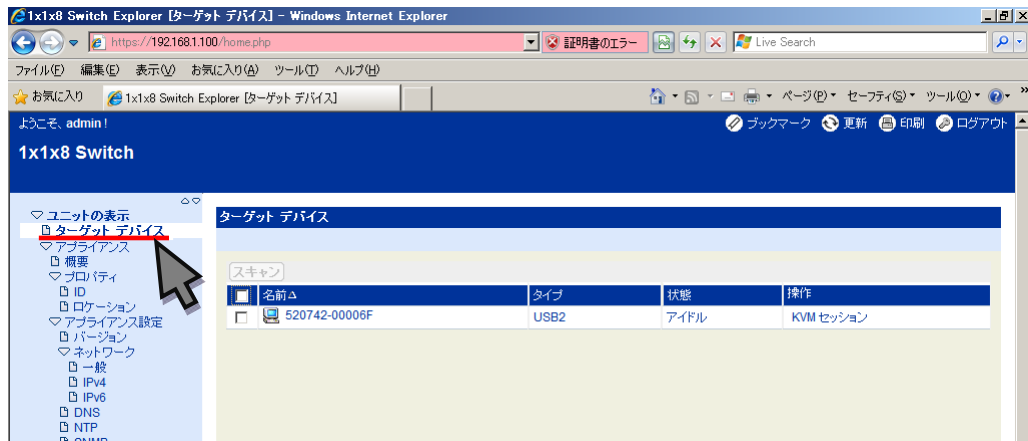
本製品は初期状態で **サーバーユニットの自動アップグレードが有効** になっております。アップグレード時間はサーバーユニット毎に約 7 分かかりますが、その間、**本体側の電源を切らないようお願い致します。**自動アップグレードの対象は DSM02 シリーズのサーバユニットとなります。本製品に取り付けの際は予めご了承ください。

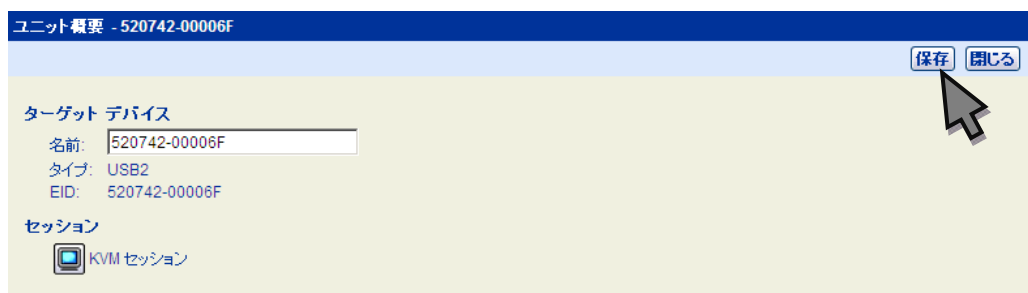
📖 参照 3.18.3 サーバーユニットのアップグレード（109 ページ）

⑥ Java のアプリケーションが起動します。下のように警告ダイアログが表示される場合は、「実行」ボタンをクリックします。

⑦ 下のようなビデオセッションビューア画面が表示され、ターゲットデバイスの操作が可能となります。

ビデオセッションビューアの詳細内容については、以下の章をご参照ください。

参照 Chapter 4 - ビデオセッションビューア（167 ページ）

3.5. ターゲットデバイスの名称変更

画面左のメニュー選択領域において、「ユニットの表示」-「ターゲットデバイス」をクリックすると「ターゲットデバイス」ページが表示されます。下のように現在接続されている、あるいは、以前接続されたことがあるサーバーユニットがリスト表示されます。

サーバーユニットに設定された名称を変更する場合、その名称をクリックします。

下のようなページが表示されます。名前に任意の名称を入力し、右上の[保存]ボタンをクリックすると変更が反映されます。

本変更は、OBWI 上で表記されるの全てのターゲットデバイス名称に反映されます。

重要

ターゲットの名前は 1～15 文字としてください。 3.6.12 工場出荷時状態へのリセット(82ページ)を実行したとき、サーバユニットの仕様によりターゲットデバイスの名称のうち 16 文字以降が消去されます。

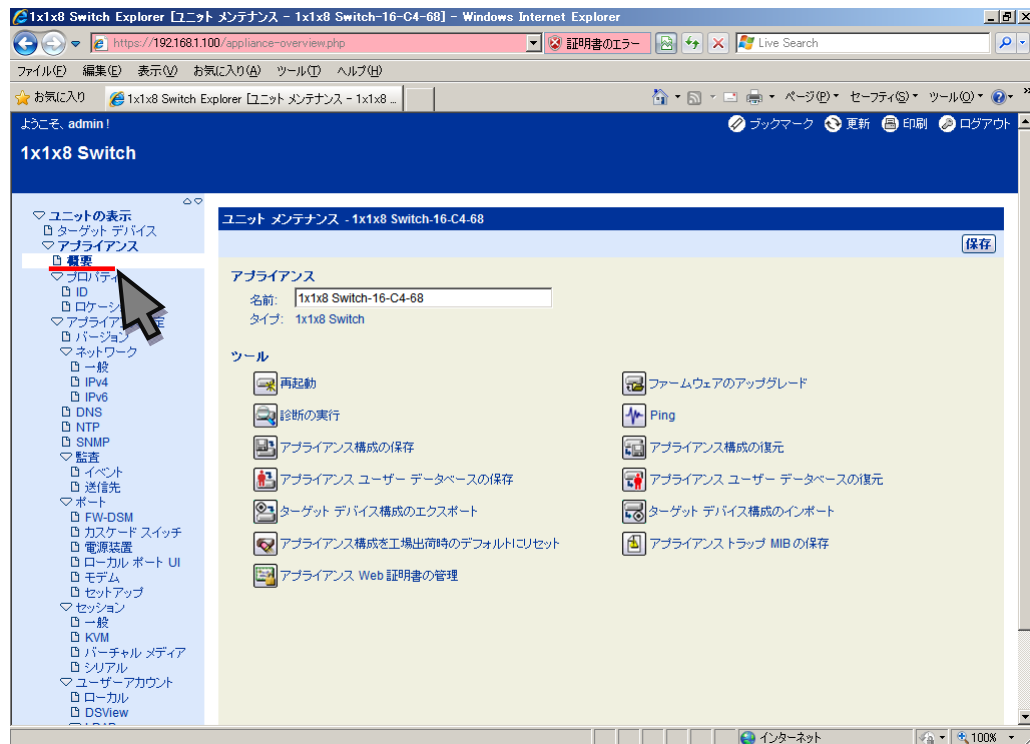
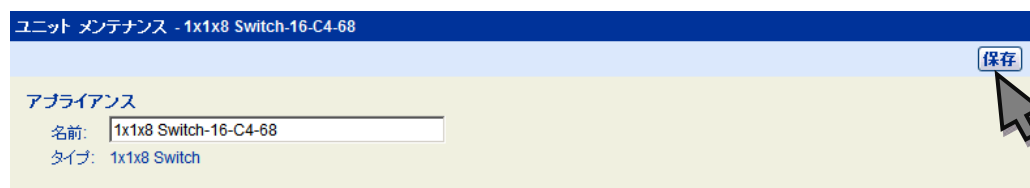
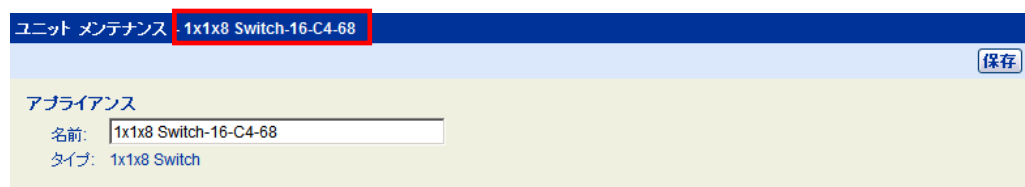
3.6. ユニットメンテナンス

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると「ユニットメンテナンス」ページが表示されます。設定保存などに関する各種ツールを使用することができます。

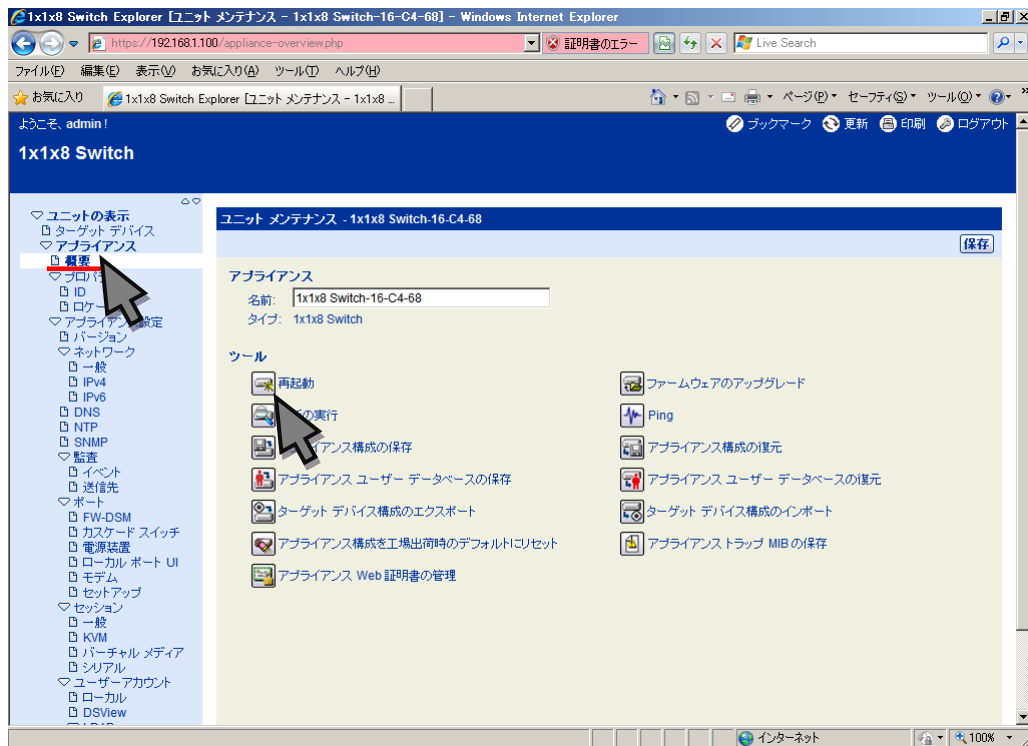
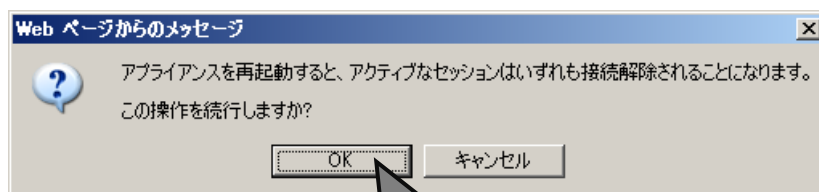
ツール項目の概要について、以下に示します。詳細については、次項から説明します。

ツール項目	内容
再起動	本装置を再起動します。
ファームウェアのアップグレード	本装置のファームウェアをアップグレードします。
診断の実行	本装置の現在のハードウェア状態を確認します。
Ping	ネットワーク上の任意のアドレスに対して Ping 送信します。
アプライアンス構成の保存	本装置の構成をファイルに保存します。
アプライアンス構成の復元	あらかじめ保存された構成ファイルを本装置に復元します。
アプライアンスユーザーデータベースの保存	本装置のユーザーデータベースを保存します。
アプライアンスユーザーデータベースの復元	あらかじめ保存されたユーザーデータベースを本装置に復元します。
ターゲットデバイス構成のエクスポート	ターゲットデバイスの構成をファイルに保存します。
ターゲットデバイス構成のインポート	あらかじめ保存されたターゲットデバイスの構成を本装置に復元します。
アプライアンス構成を工場出荷時のデフォルトにリセット	本装置の全ての設定を工場出荷時のデフォルトにリセットします。
アプライアンストラップ MIB の保存	トラップ MIB を保存します。
アプライアンス Web 証明書の管理	本装置の Web サーバー証明書に関する設定を行います。

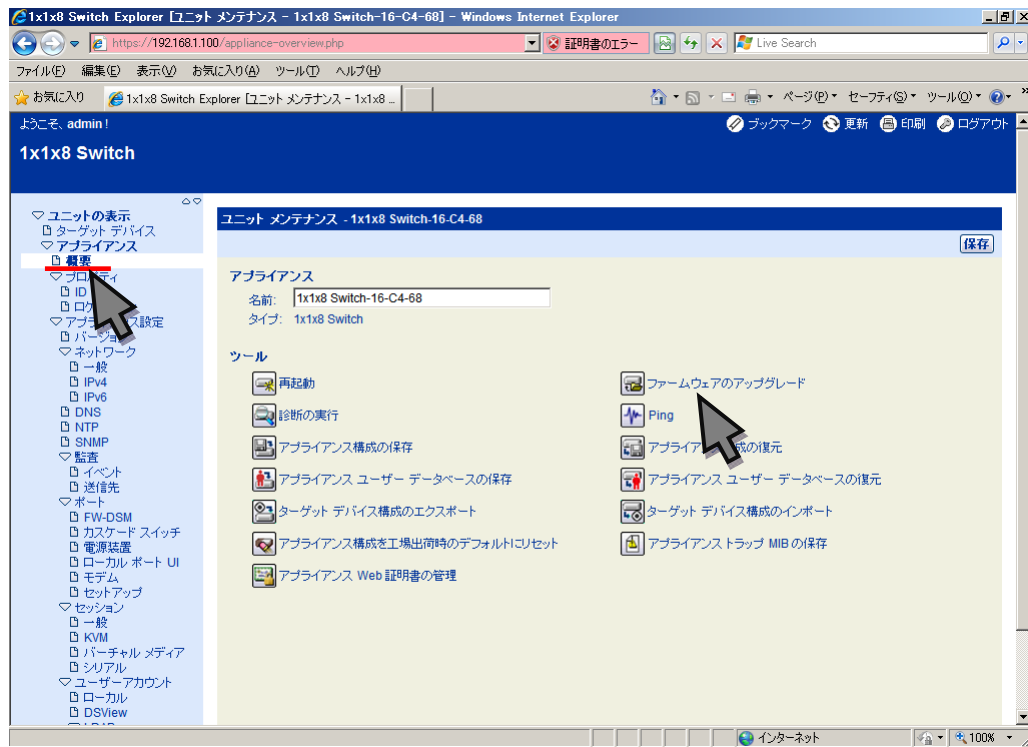
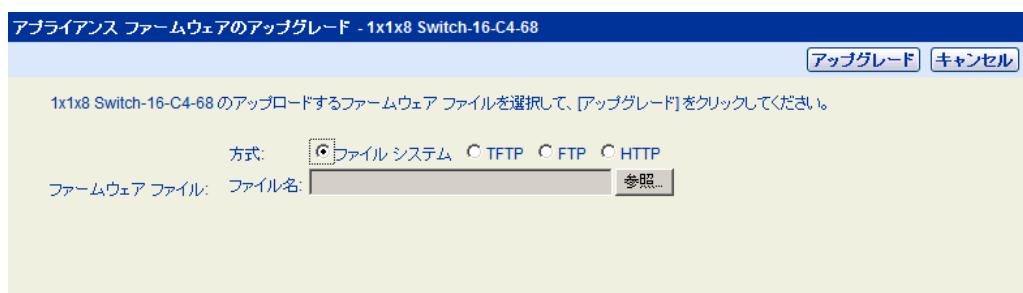
3.6.1 アプライアンスの名称設定

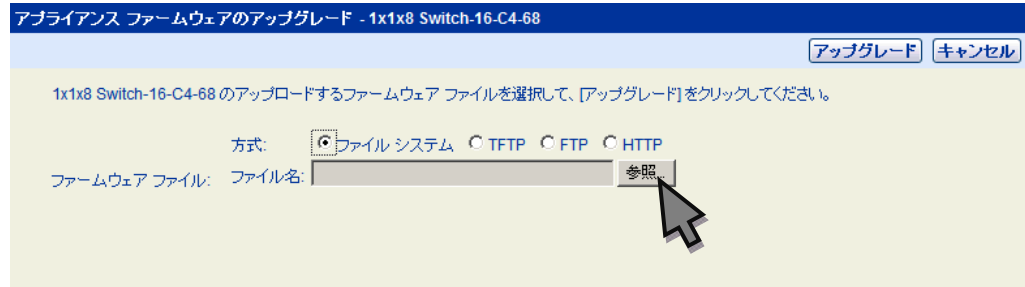
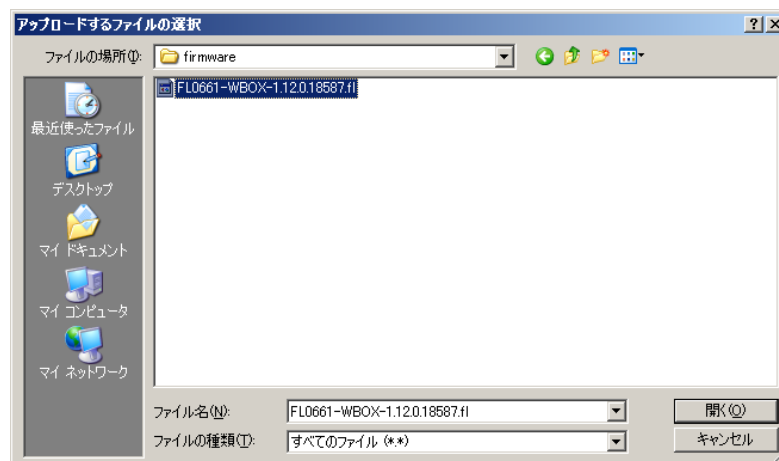
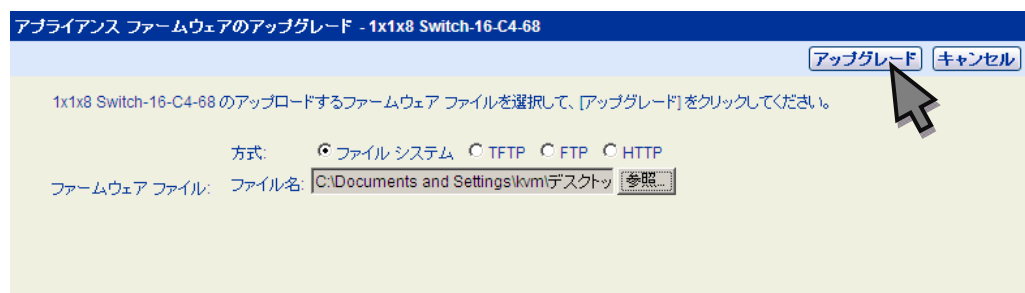
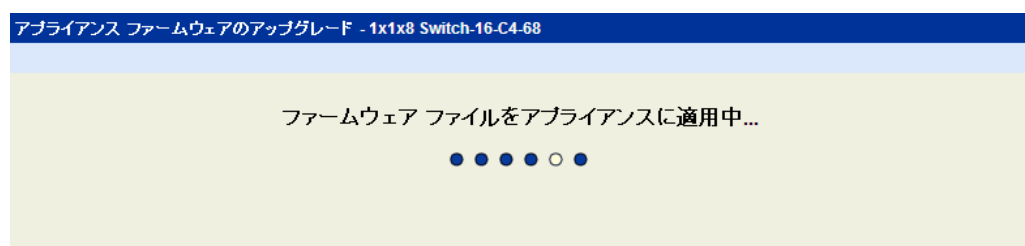
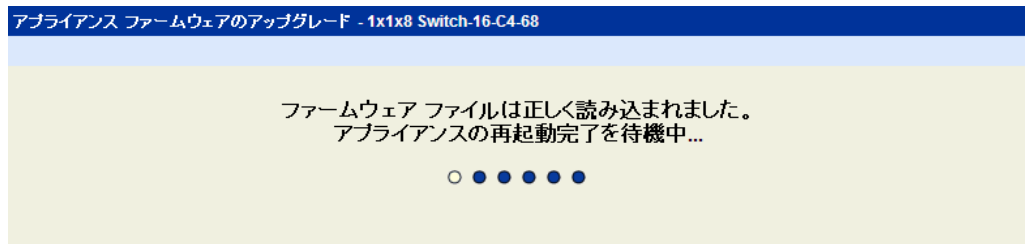
本装置に設定されている名称を変更することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。

「アプライアンス」項目の"名前" テキストボックスに任意の名称を入力し、右上の[保存]ボタンをクリックします。

アプライアンス名称は、メニュー表示領域のタイトルやタイトルバーの装置名称などに適用されます。

また、本設定は、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「SNMP」をクリックすると表示される「SNMP」ページで設定できる、システムの "名前" 設定と同一の設定値になります。どちらか一方を変更すると他方にも反映されます。

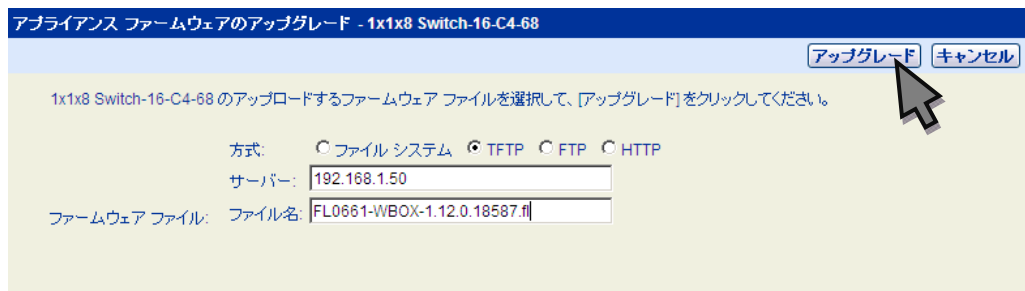
3.6.2 アプライアンスの再起動

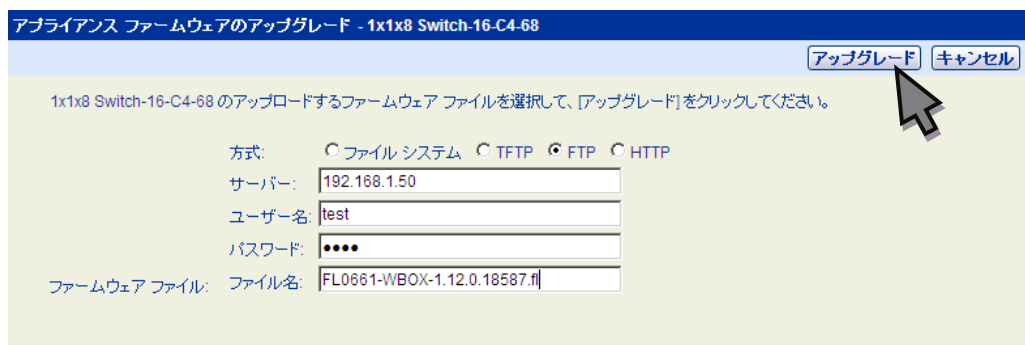
本装置を再起動させることができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。「ツール」項目の［再起動］ボタンをクリックします。

下のような確認メッセージが表示されます。［OK］ボタンをクリックします。

再起動が実行されます。約 1 分 30 秒後、本装置は起動します。

3.6.3 ファームウェアのアップグレード

本装置のファームウェアをアップグレードすることができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。「ツール」項目の[ファームウェアのアップグレード]ボタンをクリックします。

下のようなページが表示されます。ファームウェアファイルのアップロード方式をラジオボタンで選択します。

［アップロード方式が ”ファイルシステム” の場合］

”ファイルシステム” とは、OBWI アクセスしているリモート端末上に存在するファームウェアファイルを指定する場合の方式です。［参照］ボタンをクリックします。

リモート端末において、アップデートするファームウェアファイルを指定します。

右上の［アップグレード］ボタンをクリックします。

アップグレードが開始されると下のように表示されます。

アップグレードが完了すると下のように表示され、自動的に再起動されます。
再起動後、アップグレードしたファームウェアで動作します。

［アップロード方式が ”TFTP” の場合］

”TFTP” は、TFTP サーバー上に存在するファームウェアファイルを指定する場合の方式です。”TFTP” をラジオボタンで選択すると下のようなページが表示されます。
TFTP サーバーのアドレス、ファームウェアのファイル名を入力し、［アップグレード］ボタンをクリックします。

［アップロード方式が ”FTP” の場合］

”FTP” は、FTP サーバー上に存在するファームウェアファイルを指定する場合の方式です。”FTP” をラジオボタンで選択すると下のようなページが表示されます。
FTP サーバーのアドレス、FTP サーバーへアクセスするユーザー名およびパスワード、ファームウェアのファイル名を入力し、［アップグレード］ボタンをクリックします。

［アップロード方式が ”HTTP” の場合］

”HTTP” は、HTTP サーバー上に存在するファームウェアファイルを指定する場合の方式です。”HTTP” をラジオボタンで選択すると下のようなページが表示されます。
HTTP サーバーのアドレス、HTTP サーバーへアクセスするユーザー名およびパスワード、ファームウェアのファイル名を入力し、［アップグレード］ボタンをクリックします。

アプライアンス ファームウェアのアップグレード - 1x1x8 Switch-16-C4-68

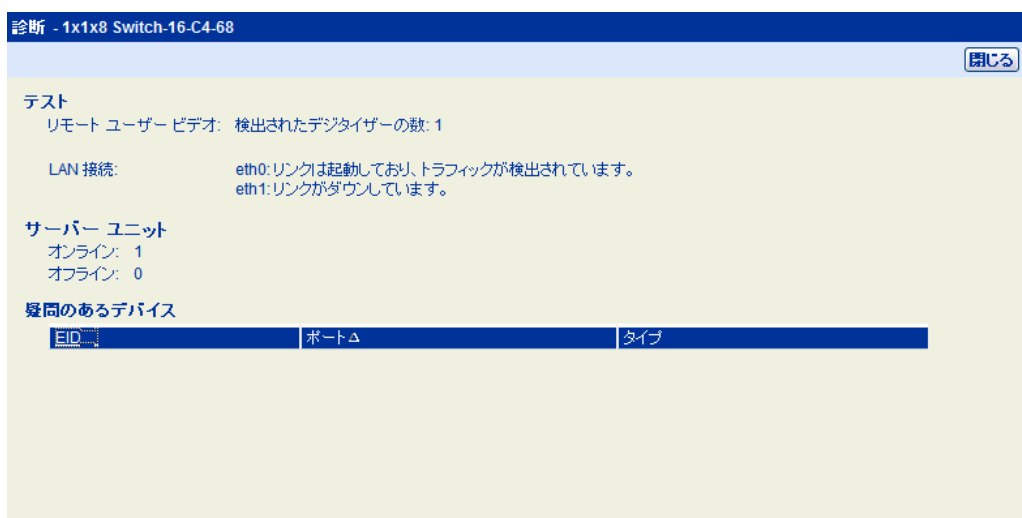
アップグレード キャンセル

1x1x8 Switch-16-C4-68 のアップロードするファームウェア ファイルを選択して、[アップグレード] をクリックしてください。

方式: ファイル システム TFTP FTP HTTP
サーバー: 192.168.1.100
ユーザー名: test
パスワード: ●●●●
ファームウェア ファイル: ファイル名: FL0661-WBOX-1.12.0.18587.fl

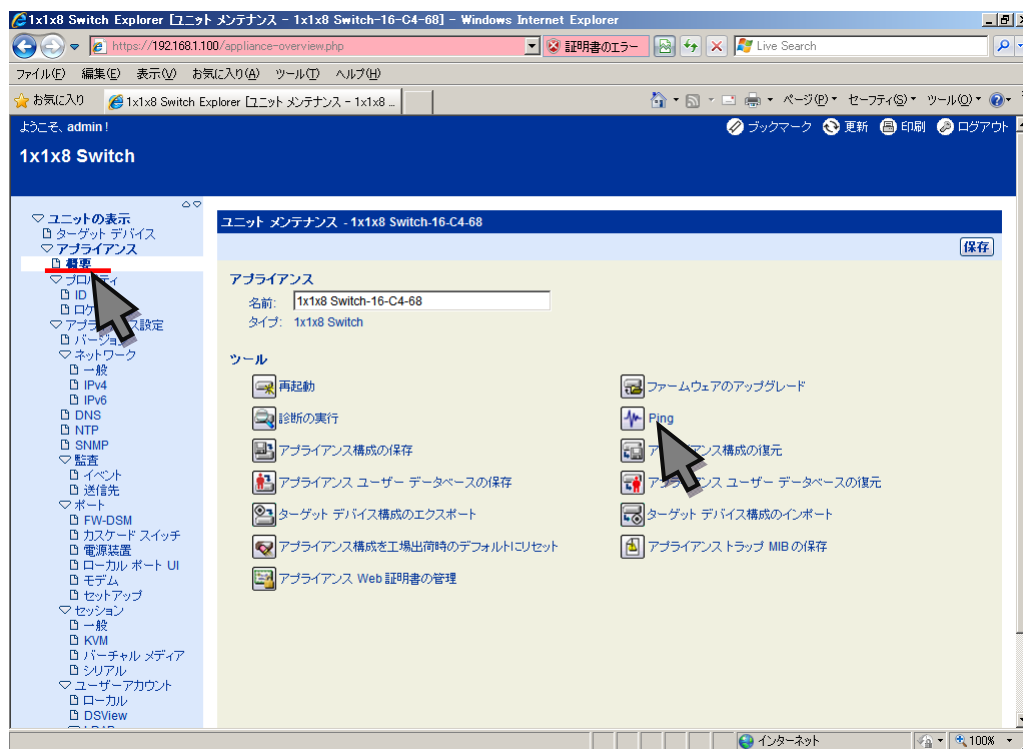
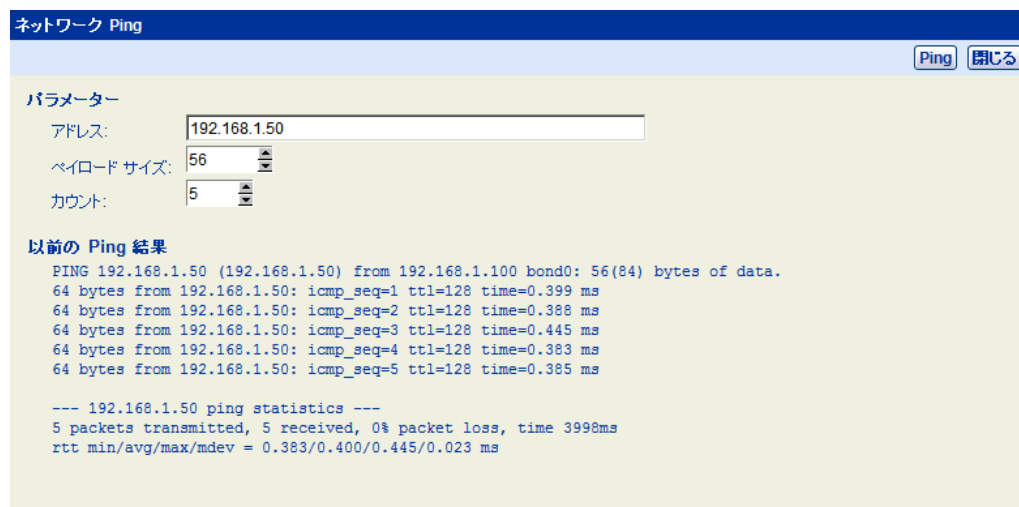
3.6.4　アプライアンスの診断

本装置のハードウェア的な状態を確認することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。「ツール」項目の［診断の実行］ボタンをクリックします。

下のようなページが表示されます。LAN ポートのリンク状態、サーバーユニットのオンライン／オフライン状態などを確認することができます。

診断表示の詳細は、下記のとおりです。

ツール項目	内容
リモートユーザービデオ	検出されたデジタイザーの数です。 FW-D1108NP は 1 FW-D2116NP は 2 FW-D8132NP は 8
LAN 接続	現在の eth0, eth1 ポートのリンク状態を示します。
サーバーユニット オンライン/オフライン	現在のサーバーユニットのオンラインあるいはオフラインの状態を示します。
疑問のあるデバイス	本装置ではサポートしていないデバイスが検出された場合などに表示されます。

3.6.5 Ping 送信

本装置からネットワーク上のアドレスに対して Ping 送信を実行することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。[Ping]ボタンをクリックします。

下のようなページが表示されます。「パラメーター」項目の "アドレス"、"ペイロード サイズ"、"カウント" をそれぞれ指定し、右上の[Ping]ボタンをクリックします。

項	設定項目	内容
1	アドレス	パケットの送信先アドレスを指定します。
2	ペイロードサイズ	送信パケットデータのサイズを指定します。0～65535 バイトの範囲で指定することができます。
3	カウント	パケットの送信回数を指定します。1～10 回の範囲で指定することができます。

Ping の送信結果が下のように表示されます。

3.6.6 アプライアンス構成の保存

本装置の設定内容を保存することができます。また、保存先を指定することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。[アプライアンス構成の保存]ボタンをクリックします。

重要

本機能では下記に示すメニュー内の設定値(下線部) は保存されません。

アプライアンス → 概要 → アプライアンスの名称
アプライアンス → アプライアンス設定 → ネットワーク
アプライアンスの設定 → SNMP
アプライアンスの設定 → 監査 → イベント
アプライアンスの設定 → セッション → KVM
アプライアンスの設定 → セッション → バーチャルメディア
アプライアンスの設定 → セッション → バーチャルメディア
アプライアンスの設定 → ユーザアカウント → バ LDAP

［保存先が ”ファイルシステム” の場合］

”ファイルシステム” とは、OBWI アクセスしているリモート端末上にファイルを保存する場合の方式です。”ファイルシステム” をラジオボタンで選択すると下のようなページが表示されます。”暗号化パスワード” は、「アプライアンス構成の復元」の際に用いるパスワードを指定します。”暗号化パスワード” は省略することもできます。入力後、［ダウンロード］ボタンをクリックします。

構成ファイルの保存が開始されると下のように表示されます。

下のようなウィンドウが表示されます。保存場所を指定します。

構成ファイルの保存が完了すると下のように表示されます。［閉じる］ボタンをクリックすると「ユニットメンテナンス」ページに戻ります。

［保存先方式が ”TFTP” の場合］

”TFTP” は、TFTP サーバー上にファイルを保存する場合の方式です。
”TFTP” をラジオボタンで選択すると下のようなページが表示されます。
TFTP サーバーのアドレス、構成ファイル名、構成ファイルの復元の際に使用する暗号化パスワード（省略可）を入力し、［ダウンロード］ボタンをクリックします。

アプライアンス構成の保存 - 1x1x8 Switch-16-C4-68
[ダウンロード] [キャンセル]
1x1x8 Switch-16-C4-68 のアプライアンス構成ファイルを保存する場所を選択してください。
方式: ○ファイル システム ◉TFTP ○FTP ○HTTP PUT
サーバー: 192.168.1.50
構成ファイル: ファイル名: conf_data
暗号化パスワード:

［保存先方式が ”FTP” の場合］

”FTP” は、FTP サーバー上にファイルを保存する場合の方式です。
”FTP” をラジオボタンで選択すると下のようなページが表示されます。
FTP サーバーのアドレス、FTP サーバーへアクセスするユーザー名およびパスワード、構成ファイル名、構成ファイルの復元の際に使用する暗号化パスワード（省略可）を入力し、［ダウンロード］ボタンをクリックします。

アプライアンス構成の保存 - 1x1x8 Switch-16-C4-68
[ダウンロード] [キャンセル]
1x1x8 Switch-16-C4-68 のアプライアンス構成ファイルを保存する場所を選択してください。
方式: ○ファイル システム ○TFTP ◉FTP ○HTTP PUT
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ●●●●
構成ファイル: ファイル名: conf_data
暗号化パスワード:

［保存先方式が ”HTTP” の場合］

”HTTP” は、HTTP サーバー上にファイルを保存する場合の方式です。
”HTTP” をラジオボタンで選択すると下のようなページが表示されます。
HTTP サーバーのアドレス、HTTP サーバーへアクセスするユーザー名およびパスワード、構成ファイル名、構成ファイルの復元の際に使用する暗号化パスワード（省略可）を入力し、[ダウンロード]ボタンをクリックします。

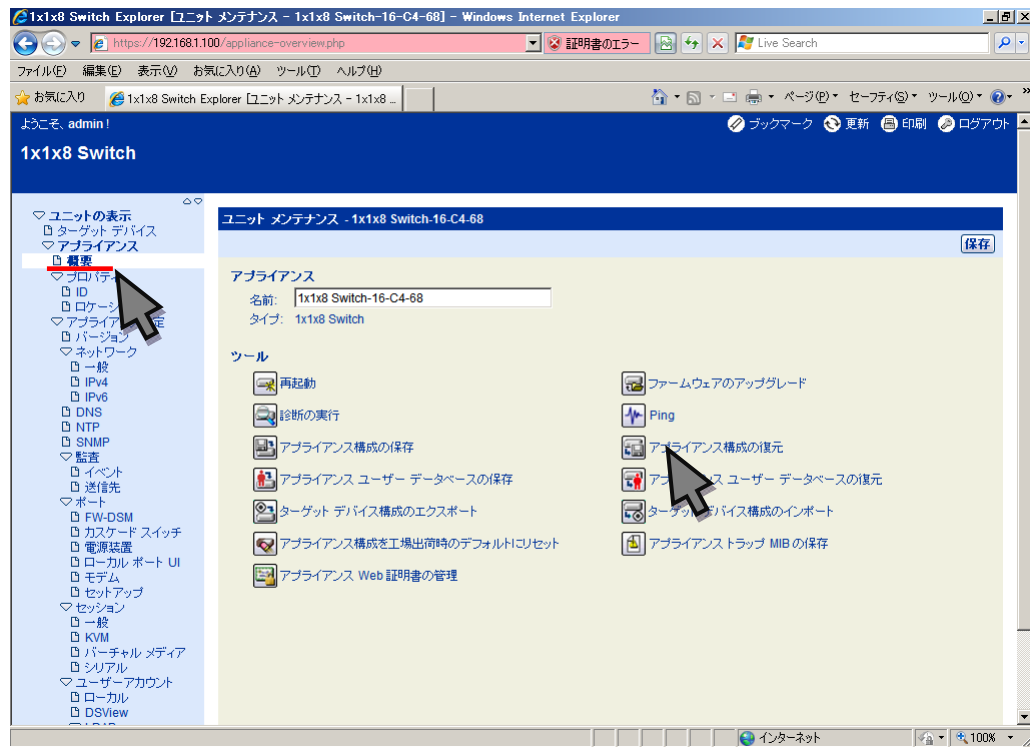
アプライアンス構成の保存 - 1x1x8 Switch-16-C4-68

[ダウンロード] [キャンセル]

1x1x8 Switch-16-C4-68 のアプライアンス構成ファイルを保存する場所を選択してください。

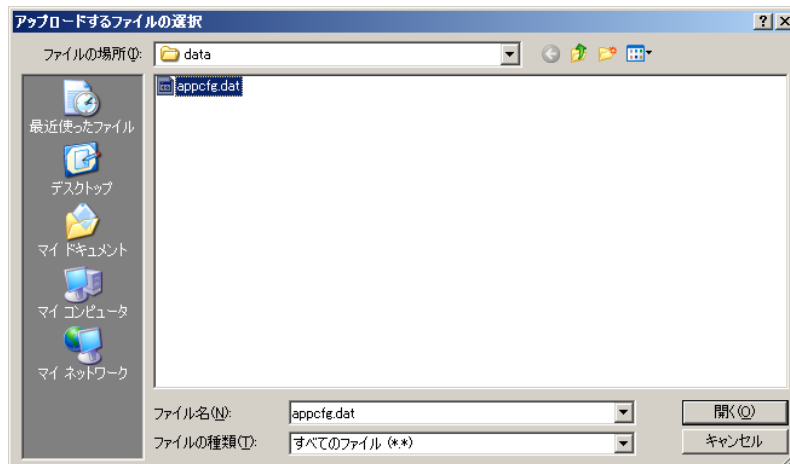
	方式:	○ファイル システム ○TFTP ○FTP ◉HTTP PUT
	サーバー:	192.168.1.50
	ユーザー名:	test
	パスワード:	●●●●
構成ファイル:	ファイル名:	conf_data
暗号化パスワード:		

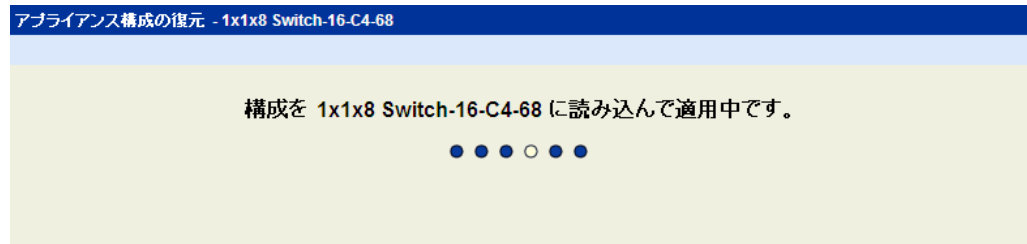
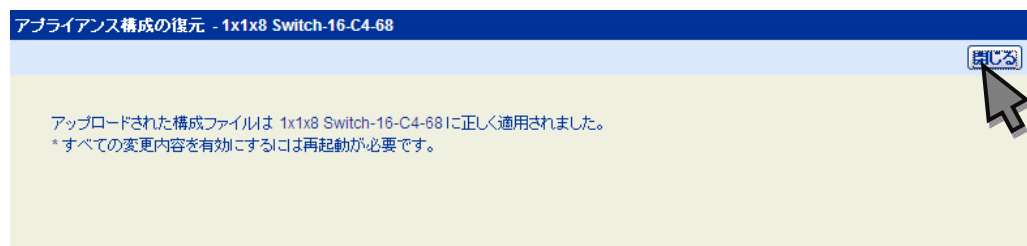
3.6.7　アプライアンス構成の復元

あらかじめ保存しておいた本装置の設定内容を読み込んで、復元することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。[アプライアンス構成の復元]ボタンをクリックします。

下のようなページが表示されます。アプライアンス構成ファイルの読み込み方式をラジオボタンで選択します。

［読み込み先が ”ファイルシステム” の場合］

”ファイルシステム” とは、OBWI アクセスしているリモート端末上に読み込む構成ファイルが存在する場合の方式です。”ファイルシステム” をラジオボタンで選択すると下のようなページが表示されます。［参照］ボタンをクリックします。

下のようなウィンドウが表示されます。読み込むファイルを指定します。

”暗号化解除パスワード” には、「アプライアンス構成の保存」の際に設定したパスワードを指定します（未設定の場合は、空白）。入力後、［アップロード］ボタンをクリックします。

構成ファイルの復元が開始されると下のように表示されます。

構成ファイルの復元が完了すると下のように表示されます。[閉じる]ボタンをクリックすると「ユニットメンテナンス」ページに戻ります。

全ての変更内容を有効にするには、本装置の再起動が必要です。

［読み込み先が ”TFTP” の場合］

”TFTP” は、TFTP サーバー上に読み込む構成ファイルが存在する場合の方式です。
”TFTP” をラジオボタンで選択すると下のようなページが表示されます。
TFTP サーバーのアドレス、構成ファイル名、「構成ファイルの保存」の際に設定した暗号化パスワード（未設定の場合は、空白）を入力し、［アップロード］ボタンをクリックします。

アプライアンス構成の復元 - 1x1x8 Switch-16-C4-68
アップロード キャンセル
1x1x8 Switch-16-C4-68 に読み込むアプライアンス構成ファイルを選択してください。
方式: ○ファイル システム ◉TFTP ○FTP ○HTTP
サーバー: 192.168.1.50
構成ファイル: ファイル名: appcfg.dat
暗号化解除パスワード:

［読み込み先が ”FTP” の場合］

”FTP” は、FTP サーバー上に読み込む構成ファイルが存在する場合の方式です。
”FTP” をラジオボタンで選択すると下のようなページが表示されます。
FTP サーバーのアドレス、FTP サーバーへアクセスするユーザー名およびパスワード、構成ファイル名、「構成ファイルの保存」の際に設定した暗号化パスワード（未設定の場合は、空白）を入力し、［アップロード］ボタンをクリックします。

アプライアンス構成の復元 - 1x1x8 Switch-16-C4-68

アップロード　キャンセル

1x1x8 Switch-16-C4-68 に読み込むアプライアンス構成ファイルを選択してください。

方式:　ファイル システム　TFTP　FTP　HTTP
サーバー:　192.168.1.50
ユーザー名:　test
パスワード:　••••
構成ファイル:　ファイル名:　appcfg.dat
暗号化解除パスワード:

［読み込み先が ”HTTP” の場合］

”HTTP” は、HTTP サーバー上に読み込む構成ファイルが存在する場合の方式です。
”HTTP” をラジオボタンで選択すると下のようなページが表示されます。
HTTP サーバーのアドレス、HTTP サーバーへアクセスするユーザー名およびパスワード、構成ファイル名、「構成ファイルの保存」の際に設定した暗号化パスワード（未設定の場合は、空白）を入力し、［アップロード］ボタンをクリックします。

アプライアンス構成の復元 - 1x1x8 Switch-16-C4-68

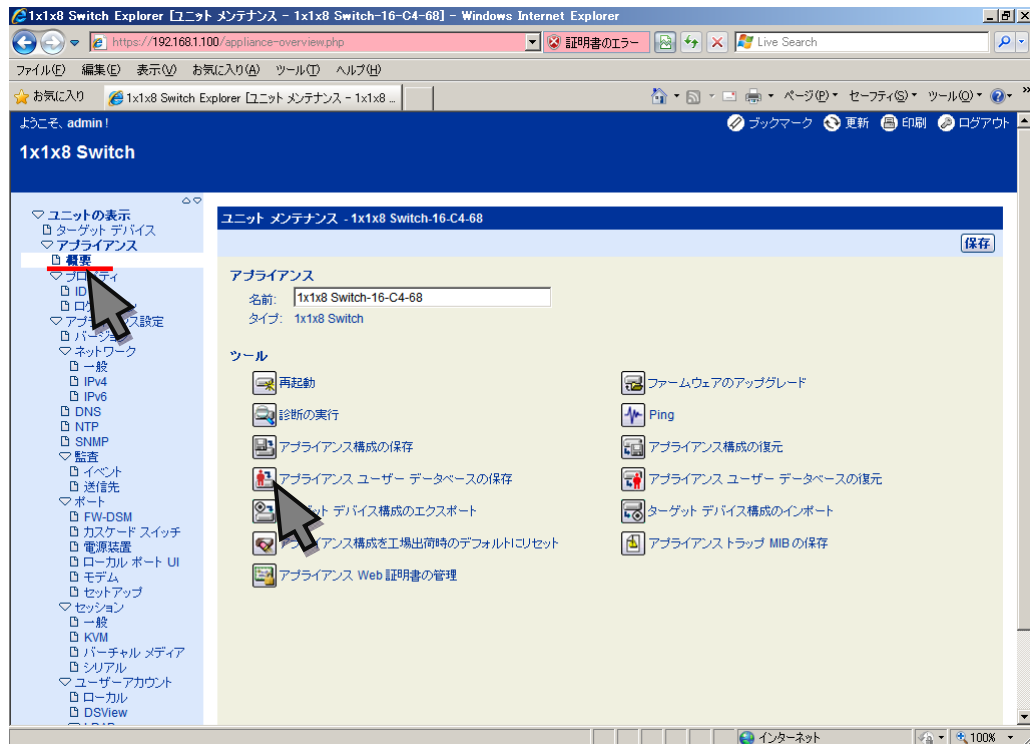
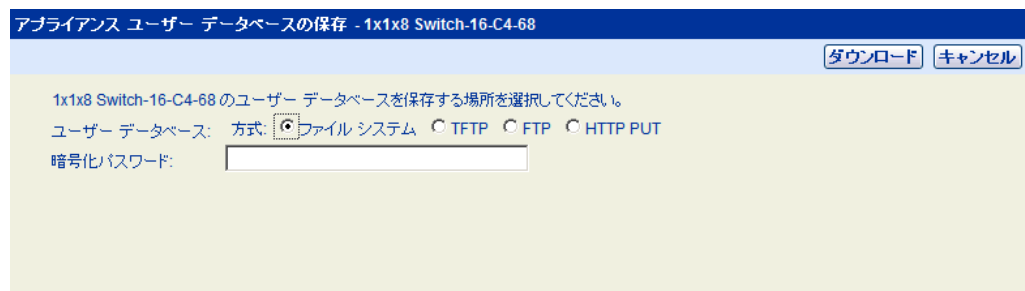
d

アップロード　キャンセル

1x1x8 Switch-16-C4-68 に読み込むアプライアンス構成ファイルを選択してください。

方式:　ファイル システム　TFTP　FTP　HTTP
サーバー:　192.168.1.50
ユーザー名:　test
パスワード:　••••
構成ファイル:　ファイル名:　appcfg.dat
暗号化解除パスワード:

3.6.8　アプライアンスユーザーデータベースの保存

本装置に設定されているユーザーデータベースを保存することができます。また、保存先を指定することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。[アプライアンスユーザーデータベースの保存]ボタンをクリックします。

下のようなページが表示されます。ユーザーデータベースファイルの保存方式をラジオボタンで選択します。

アプライアンス ユーザー データベースの保存 - 1x1x8 Switch-16-C4-68

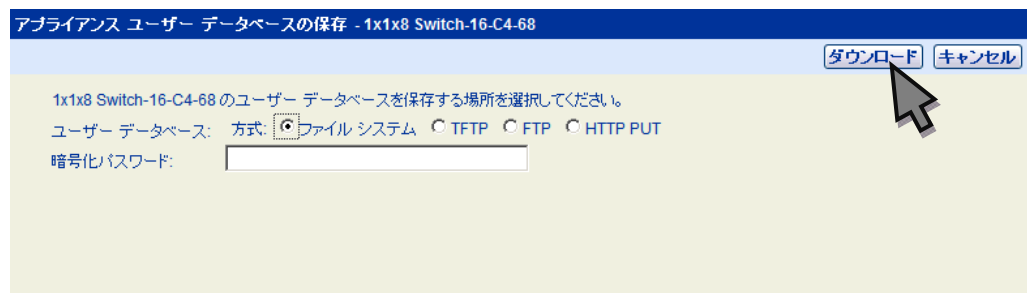
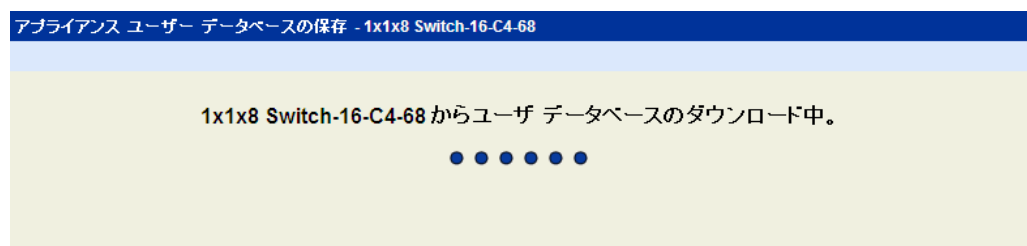
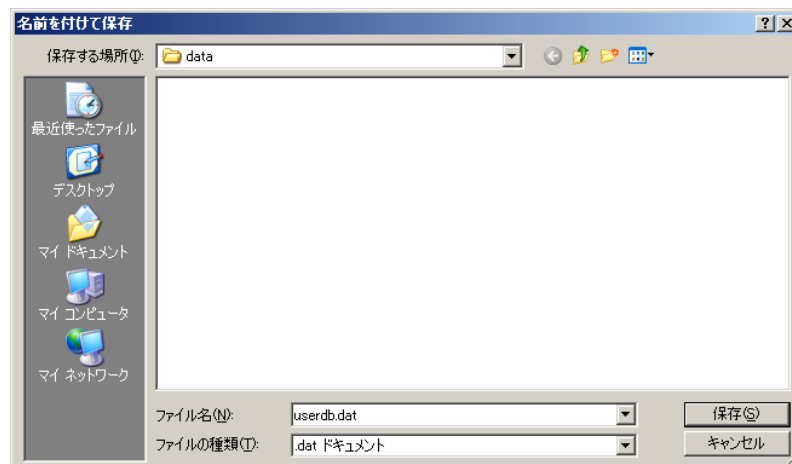
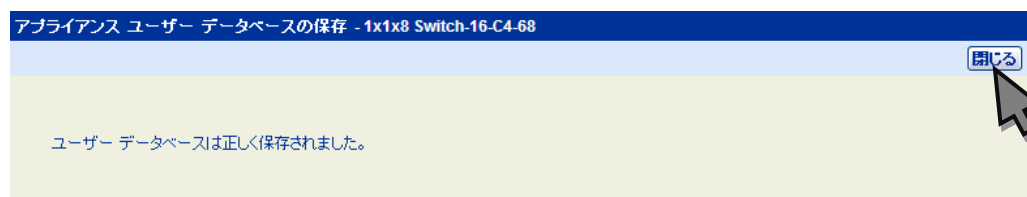
[ダウンロード] [キャンセル]

1x1x8 Switch-16-C4-68 のユーザー データベースを保存する場所を選択してください。

ユーザー データベース:　方式: ◉ファイル システム　○TFTP　○FTP　○HTTP PUT

暗号化パスワード:

[保存先が ”ファイルシステム” の場合]

”ファイルシステム” とは、OBWI アクセスしているリモート端末上にファイルを保存する場合の方式です。”ファイルシステム” をラジオボタンで選択すると下のようなページが表示されます。”暗号化パスワード” は、「アプライアンスユーザーデータベースの復元」の際に用いるパスワードを指定します。”暗号化パスワード” は省略することもできます。入力後、[ダウンロード]ボタンをクリックします。

ユーザーデータベースファイルの保存が開始されると下のように表示されます。

下のようなウィンドウが表示されます。保存場所を指定します。

ユーザーデータベースファイルの保存が完了すると下のように表示されます。[閉じる]ボタンをクリックすると「ユニットメンテナンス」ページに戻ります。

［保存先方式が ”TFTP” の場合］

”TFTP” は、TFTP サーバー上にファイルを保存する場合の方式です。
”TFTP” をラジオボタンで選択すると下のようなページが表示されます。TFTP サーバーのアドレス、保存ファイル名、「アプライアンスユーザーデータベースの復元」の際に使用する暗号化パスワード（省略可）を入力し、[ダウンロード]ボタンをクリックします。

アプライアンス ユーザー データベースの保存 - 1x1x8 Switch-16-C4-68
ダウンロード キャンセル
1x1x8 Switch-16-C4-68 のユーザー データベースを保存する場所を選択してください。
方式: ファイル システム TFTP FTP HTTP PUT
サーバー: 192.168.1.50
ユーザー データベース: ファイル名: user_data
暗号化パスワード:

［保存先方式が ”FTP” の場合］

”FTP” は、FTP サーバー上にファイルを保存する場合の方式です。
”FTP” をラジオボタンで選択すると下のようなページが表示されます。FTP サーバーのアドレス、FTP サーバーへアクセスするユーザー名およびパスワード、保存ファイル名、「アプライアンスユーザーデータベースの復元」の際に使用する暗号化パスワード（省略可）を入力し、[ダウンロード]ボタンをクリックします。

アプライアンス ユーザー データベースの保存 - 1x1x8 Switch-16-C4-68
ダウンロード キャンセル
1x1x8 Switch-16-C4-68 のユーザー データベースを保存する場所を選択してください。
方式: ファイル システム TFTP FTP HTTP PUT
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ••••
ユーザー データベース: ファイル名: user_data
暗号化パスワード:

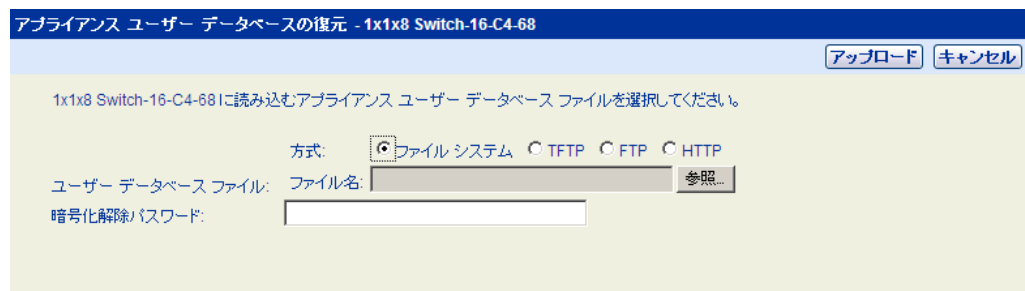
［保存先方式が ”HTTP” の場合］

”HTTP” は、HTTP サーバー上にファイルを保存する場合の方式です。
”HTTP” をラジオボタンで選択すると下のようなページが表示されます。
HTTP サーバーのアドレス、HTTP サーバーへアクセスするユーザー名およびパスワード、保存ファイル名、「アプライアンスユーザーデータベースの復元」の際に使用する暗号化パスワード（省略可）を入力し、［ダウンロード］ボタンをクリックします。

アプライアンス ユーザー データベースの保存 - 1x1x8 Switch-16-C4-68
ダウンロード キャンセル
1x1x8 Switch-16-C4-68 のユーザー データベースを保存する場所を選択してください。
方式: ファイル システム TFTP FTP HTTP PUT
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ●●●●
ユーザー データベース: ファイル名: user_data
暗号化パスワード:

3.6.9　アプライアンスユーザーデータベースの復元

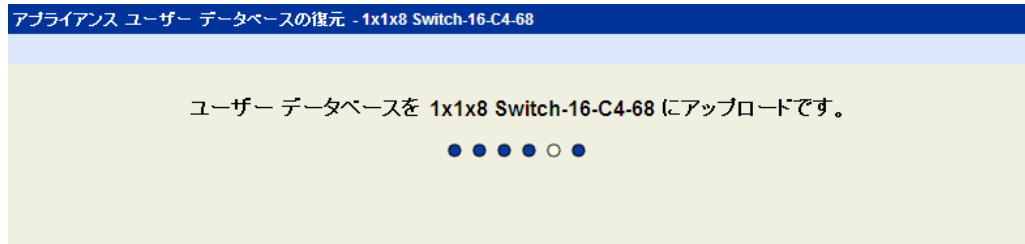
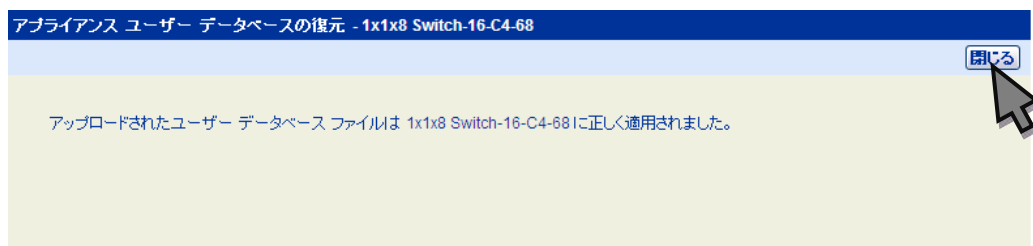
あらかじめ保存しておいた本装置のユーザーデータベースの内容を読み込んで、復元することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。[アプライアンスユーザーデータベースの復元]ボタンをクリックします。

下のようなページが表示されます。ユーザーデータベースファイルの読み込み方式をラジオボタンで選択します。

［読み込み先が ”ファイルシステム” の場合］

”ファイルシステム” とは、OBWI アクセスしているリモート端末上に読み込むユーザーデータベースファイルが存在する場合の方式です。”ファイルシステム” をラジオボタンで選択すると下のようなページが表示されます。［参照］ボタンをクリックします。

下のようなウィンドウが表示されます。読み込むファイルを指定します。

”暗号化解除パスワード” は、「アプライアンスユーザーデータベースの保存」の際に設定したパスワードを指定します（未設定の場合は、空白）。入力後、［アップロード］ボタンをクリックします。

ユーザーデータベースファイルの復元が開始されると下のように表示されます。

ユーザーデータベースファイルの復元が完了すると下のように表示されます。[閉じる]ボタンをクリックすると「ユニットメンテナンス」ページに戻ります。

［読み込み先が ”TFTP” の場合］

”TFTP” は、TFTP サーバー上に読み込むユーザーデータベースファイルが存在する場合の方式です。”TFTP” をラジオボタンで選択すると下のようなページが表示されます。TFTP サーバーのアドレス、ファイル名、「アプライアンスユーザーデータベースの保存」の際に設定した暗号化パスワード（未設定の場合は、空白）を入力し、[アップロード]ボタンをクリックします。

アプライアンス ユーザー データベースの復元 - 1x1x8 Switch-16-C4-68
アップロード キャンセル
1x1x8 Switch-16-C4-68 に読み込むアプライアンス ユーザー データベース ファイルを選択してください。
方式: ファイル システム TFTP FTP HTTP
ユーザー データベース ファイル: サーバー: 192.168.1.50
ファイル名: user_data
暗号化解除パスワード:

［読み込み先が ”FTP” の場合］

”FTP” は、FTP サーバー上に読み込むユーザーデータベースファイルが存在する場合の方式です。”FTP” をラジオボタンで選択すると下のようなページが表示されます。
FTP サーバーのアドレス、FTP サーバーへアクセスするユーザー名およびパスワード、ファイル名、「アプライアンスユーザーデータベースの保存」の際に設定した暗号化パスワード（未設定の場合は、空白）を入力し、［アップロード］ボタンをクリックします。

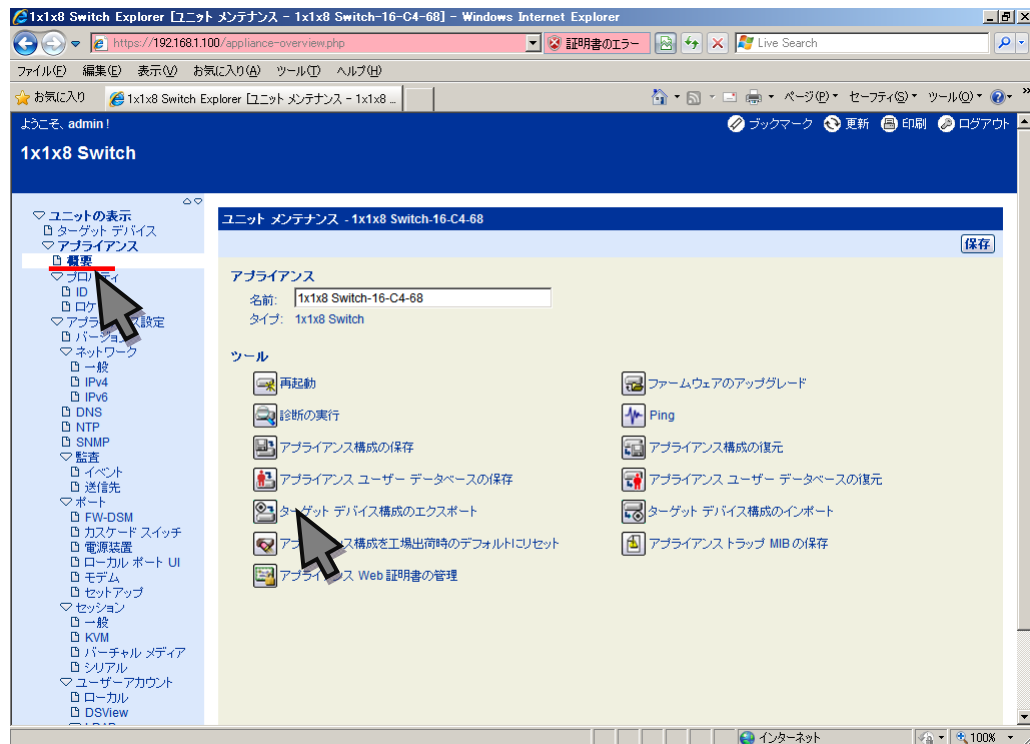
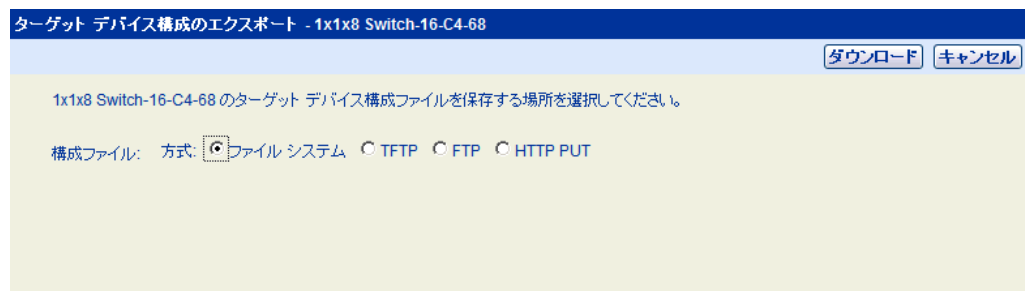
アプライアンス ユーザー データベースの復元 - 1x1x8 Switch-16-C4-68
アップロード キャンセル
1x1x8 Switch-16-C4-68 に読み込むアプライアンス ユーザー データベース ファイルを選択してください。
方式: ファイル システム TFTP FTP HTTP
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ●●●●
ユーザー データベース ファイル: ファイル名: user_data
暗号化解除パスワード:

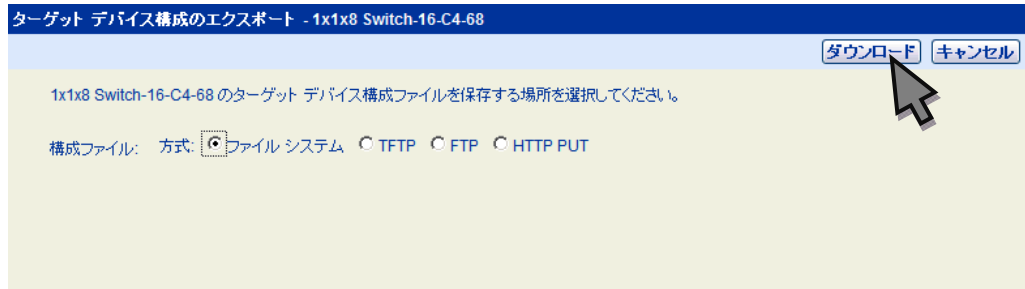
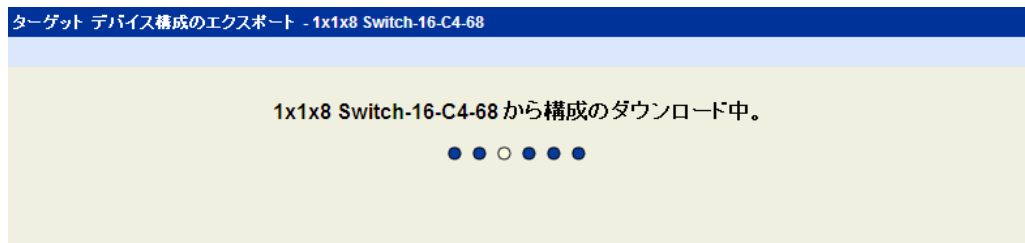
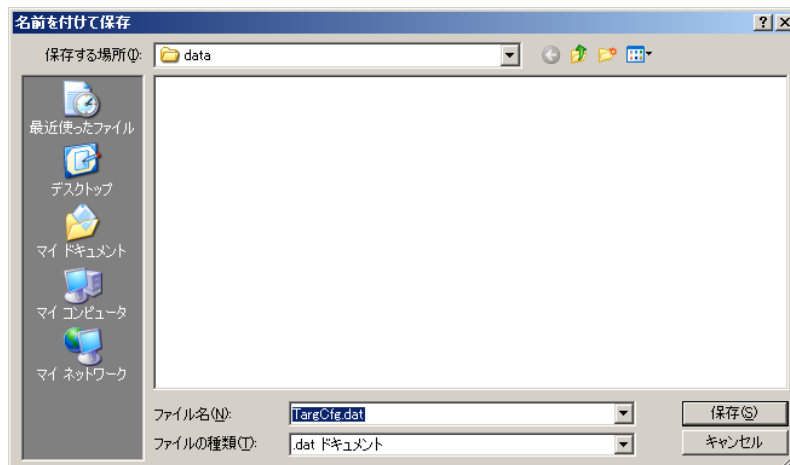
［読み込み先が ”HTTP” の場合］

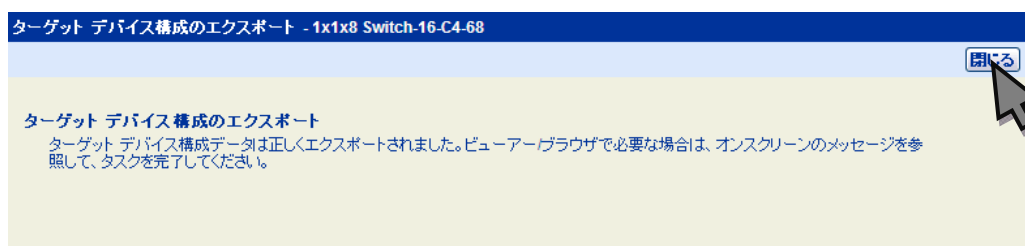
”HTTP” は、HTTP サーバー上に読み込むユーザーデータベースファイルが存在する場合の方式です。”HTTP” をラジオボタンで選択すると下のようなページが表示されます。
HTTP サーバーのアドレス、HTTP サーバーへアクセスするユーザー名およびパスワード、ファイル名、「アプライアンスユーザーデータベースの保存」の際に設定した暗号化パスワード（未設定の場合は、空白）を入力し、［アップロード］ボタンをクリックします。

アプライアンス ユーザー データベースの復元 - 1x1x8 Switch-16-C4-68
アップロード キャンセル
1x1x8 Switch-16-C4-68 に読み込むアプライアンス ユーザー データベース ファイルを選択してください。
方式: ファイル システム TFTP FTP HTTP
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ●●●●
ユーザー データベース ファイル: ファイル名: user_data
暗号化解除パスワード:

3.6.10 ターゲットデバイス構成のエクスポート

本装置に設定されているターゲットデバイス構成を保存することができます。また、保存先を指定することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。[ターゲットデバイス構成のエクスポート]ボタンをクリックします。

下のようなページが表示されます。ターゲットデバイス構成ファイルの保存方式をラジオボタンで選択します。

［保存先が ”ファイルシステム” の場合］

”ファイルシステム” とは、OBWI アクセスしているリモート端末上にファイルを保存する場合の方式です。”ファイルシステム” をラジオボタンで選択すると下のようなページが表示されます。［ダウンロード］ボタンをクリックします。

ターゲットデバイス構成ファイルの保存が開始されると下のように表示されます。

下のようなウィンドウが表示されます。保存場所を指定します。

ターゲットデバイス構成ファイルの保存が完了すると下のように表示されます。［閉じる］ボタンをクリックすると「ユニットメンテナンス」ページに戻ります。

［保存先方式が ”TFTP” の場合］

”TFTP” は、TFTP サーバー上にファイルを保存する場合の方式です。
”TFTP” をラジオボタンで選択すると下のようなページが表示されます。TFTP サーバーのアドレス、保存ファイル名を入力し、［ダウンロード］ボタンをクリックします。

ターゲット デバイス構成のエクスポート - 1x1x8 Switch-16-C4-68
ダウンロード キャンセル
1x1x8 Switch-16-C4-68 のターゲット デバイス構成ファイルを保存する場所を選択してください。
方式: ファイル システム TFTP FTP HTTP PUT
サーバー: 192.168.1.50
構成ファイル: ファイル名: target_conf

［保存先方式が ”FTP” の場合］

”FTP” は、FTP サーバー上にファイルを保存する場合の方式です。
”FTP” をラジオボタンで選択すると下のようなページが表示されます。FTP サーバーのアドレス、FTP サーバーへアクセスするユーザー名およびパスワード、保存ファイル名を入力し、［ダウンロード］ボタンをクリックします。

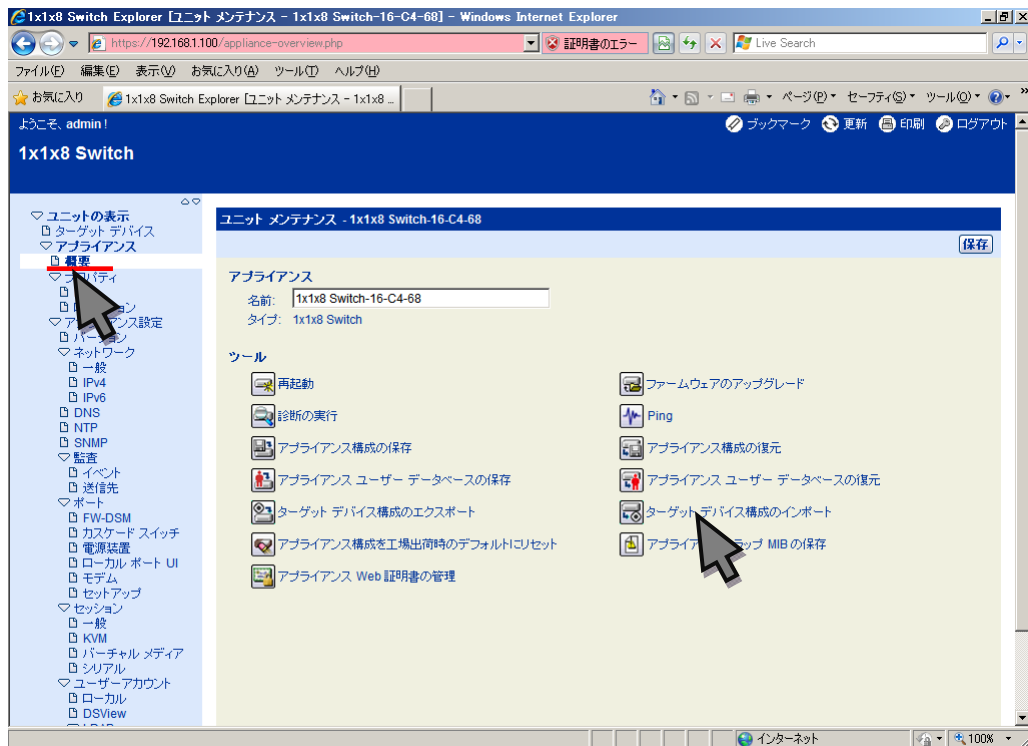
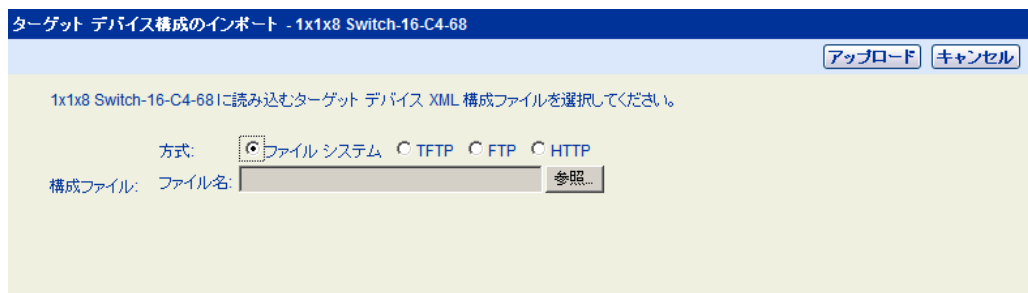
ターゲット デバイス構成のエクスポート - 1x1x8 Switch-16-C4-68
ダウンロード キャンセル
1x1x8 Switch-16-C4-68 のターゲット デバイス構成ファイルを保存する場所を選択してください。
方式: ファイル システム TFTP FTP HTTP PUT
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ••••
構成ファイル: ファイル名: target_conf

［保存先方式が ”HTTP” の場合］

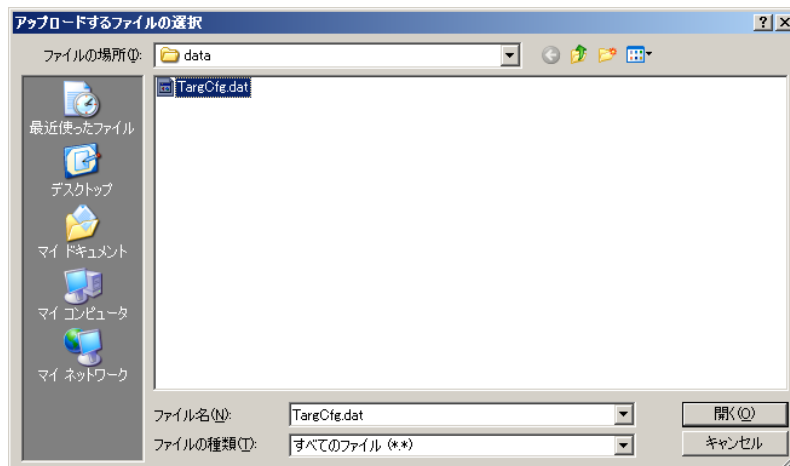
”HTTP” は、HTTP サーバー上にファイルを保存する場合の方式です。
”HTTP” をラジオボタンで選択すると下のようなページが表示されます。HTTP サーバーのアドレス、HTTP サーバーへアクセスするユーザー名およびパスワード、保存ファイル名を入力し、［ダウンロード］ボタンをクリックします。

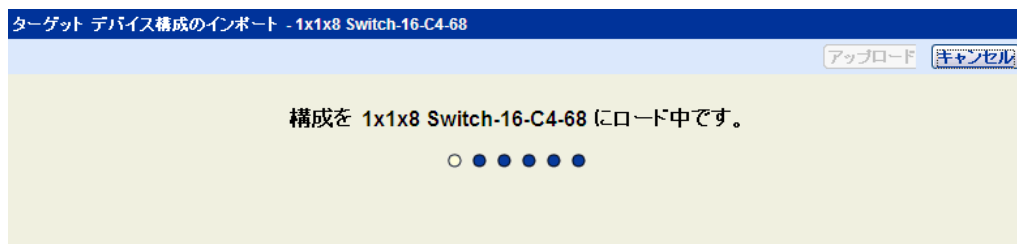
ターゲット デバイス構成のエクスポート - 1x1x8 Switch-16-C4-68
ダウンロード キャンセル
1x1x8 Switch-16-C4-68 のターゲット デバイス構成ファイルを保存する場所を選択してください。
方式: ファイル システム TFTP FTP HTTP PUT
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ••••
構成ファイル: ファイル名: target_conf

3.6.11 ターゲットデバイス構成のインポート

あらかじめ保存しておいた本装置のターゲットデバイス構成ファイルの内容を読み込むことができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。[ターゲットデバイス構成のインポート]ボタンをクリックします。

下のようなページが表示されます。ターゲットデバイス構成ファイルの読み込み方式をラジオボタンで選択します。

［読み込み先が ”ファイルシステム” の場合］

”ファイルシステム” とは、OBWI アクセスしているリモート端末上に読み込むユーザーデータベースファイルが存在する場合の方式です。”ファイルシステム” をラジオボタンで選択すると下のようなページが表示されます。[参照]ボタンをクリックします。

下のようなウィンドウが表示されます。読み込みファイルを指定します。

［アップロード］ボタンをクリックします。

ターゲットデバイス構成ファイルのインポートが開始されると下のように表示されます。

ターゲットデバイス構成ファイルのインポートが完了すると下のように表示されます。インポート操作の結果ログを確認することができます。右上の[閉じる]ボタンをクリックすると「ユニットメンテナンス」ページに戻ります。

全ての変更内容を有効にするには、再起動する必要があります。

［読み込み先が ”TFTP” の場合］

”TFTP” は、TFTP サーバー上に読み込むターゲットデバイス構成ファイルが存在する場合の方式です。”TFTP” をラジオボタンで選択すると下のようなページが表示されます。
TFTP サーバーのアドレス、ファイル名を入力し、［アップロード］ボタンをクリックします。

ターゲット デバイス構成のインポート - 1x1x8 Switch-16-C4-68
アップロード キャンセル
1x1x8 Switch-16-C4-68 に読み込むターゲット デバイス XML 構成ファイルを選択してください。
方式: ファイル システム TFTP FTP HTTP
サーバー: 192.168.1.50
構成ファイル: ファイル名: target_conf

［読み込み先が ”FTP” の場合］

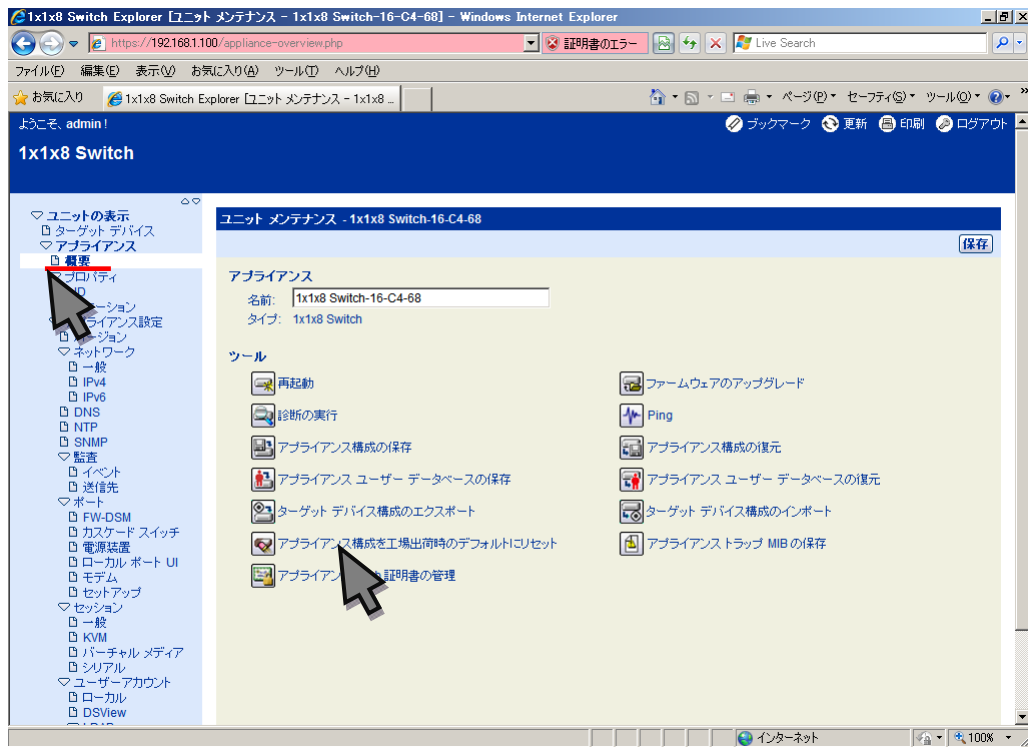
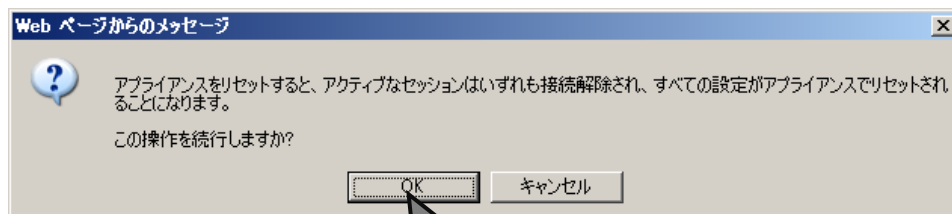
”FTP” は、FTP サーバー上に読み込むターゲットデバイス構成ファイルが存在する場合の方式です。”FTP” をラジオボタンで選択すると下のようなページが表示されます。
FTP サーバーのアドレス、FTP サーバーへアクセスするユーザー名およびパスワード、ファイル名を入力し、［アップロード］ボタンをクリックします。

ターゲット デバイス構成のインポート - 1x1x8 Switch-16-C4-68
アップロード キャンセル
1x1x8 Switch-16-C4-68 に読み込むターゲット デバイス XML 構成ファイルを選択してください。
方式: ファイル システム TFTP FTP HTTP
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ••••
構成ファイル: ファイル名: target_conf

［読み込み先が ”HTTP” の場合］

”HTTP” は、HTTP サーバー上に読み込むユーザーデータベースファイルが存在する場合の方式です。”HTTP” をラジオボタンで選択すると下のようなページが表示されます。
HTTP サーバーのアドレス、HTTP サーバーへアクセスするユーザー名およびパスワード、ファイル名を入力し、［アップロード］ボタンをクリックします。

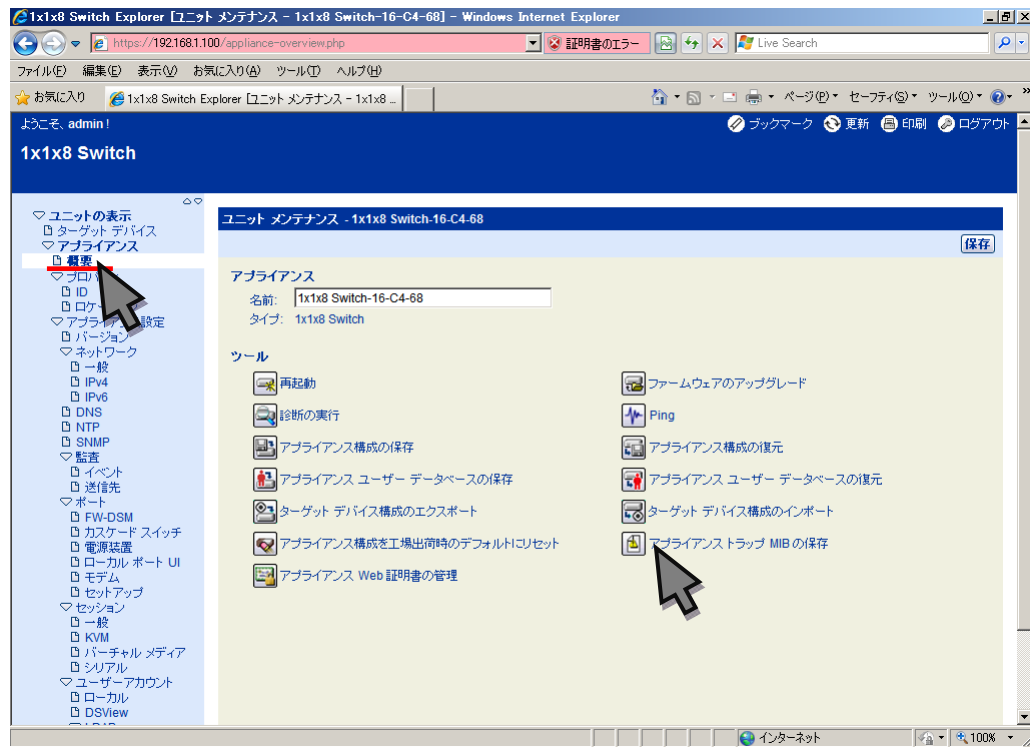
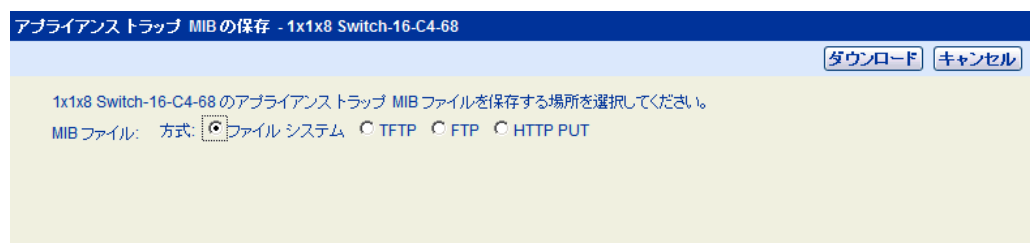
3.6.12 工場出荷時状態へのリセット

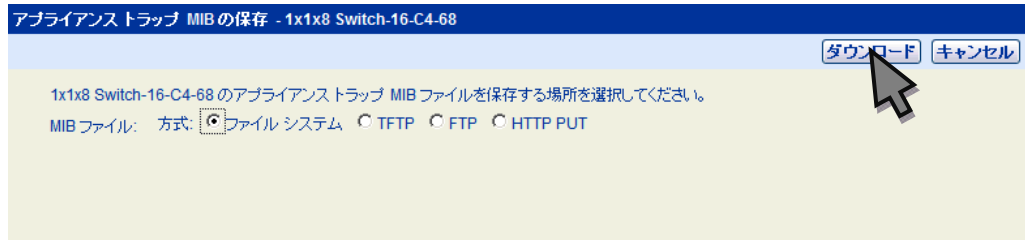
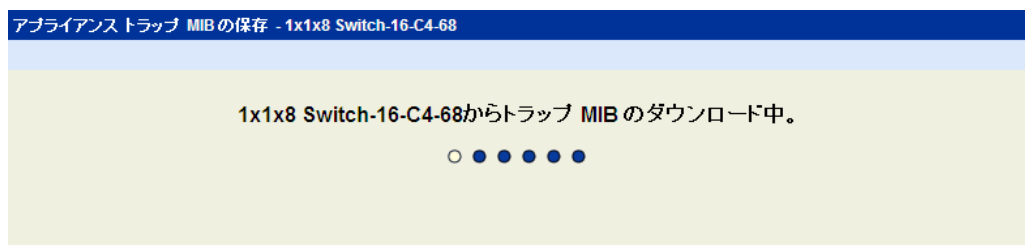
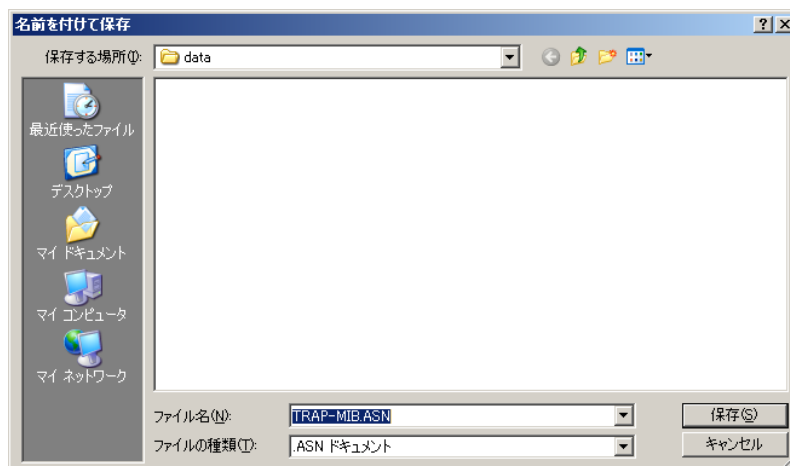
本装置を工場出荷時のデフォルト状態にリセットすることができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。[アプライアンス構成を工場出荷時のデフォルトにリセット]ボタンをクリックします。

下のような確認メッセージが表示されます。[OK]ボタンをクリックします。

リセットが実行されます。約 1 分 30 秒後、本装置は起動します。

重要

「工場出荷時のデフォルトにリセット」を実行した場合、サーバ・ユニット上の設定値のうち、名称については、15 文字以降が消去されますので、あらかじめご了承ください。

3.6.13 トラップ MIB の保存

本装置の SNMP トラップ MIB を保存することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のような「ユニットメンテナンス」ページが表示されます。[アプライアンストラップ MIB の保存]ボタンをクリックします。

下のようなページが表示されます。トラップ MIB ファイルの保存方式をラジオボタンで選択します。

［保存先が ”ファイルシステム” の場合］

”ファイルシステム” とは、OBWI アクセスしているリモート端末上にファイルを保存する場合の方式です。”ファイルシステム” をラジオボタンで選択すると下のようなページが表示されます。［ダウンロード］ボタンをクリックします。

トラップ MIB ファイルの保存が開始されると下のように表示されます。

下のようなウィンドウが表示されます。保存場所を指定します。

トラップ MIB ファイルの保存が完了すると下のように表示されます。［閉じる］ボタンをクリックすると「ユニットメンテナンス」ページに戻ります。

［保存先方式が ”TFTP” の場合］

”TFTP” は、TFTP サーバー上にファイルを保存する場合の方式です。
”TFTP” をラジオボタンで選択すると下のようなページが表示されます。TFTP サーバーのアドレス、保存ファイル名を入力し、［ダウンロード］ボタンをクリックします。

アプライアンス トラップ MIB の保存 - 1x1x8 Switch-16-C4-68
ダウンロード キャンセル
1x1x8 Switch-16-C4-68 のアプライアンス トラップ MIB ファイルを保存する場所を選択してください。
方式: ファイル システム TFTP FTP HTTP PUT
サーバー: 192.168.1.50
MIB ファイル: ファイル名: TRAP-MIB.ASN

［保存先方式が ”FTP” の場合］

”FTP” は、FTP サーバー上にファイルを保存する場合の方式です。
”FTP” をラジオボタンで選択すると下のようなページが表示されます。FTP サーバーのアドレス、FTP サーバーへアクセスするユーザー名およびパスワード、保存ファイル名を入力し、［ダウンロード］ボタンをクリックします。

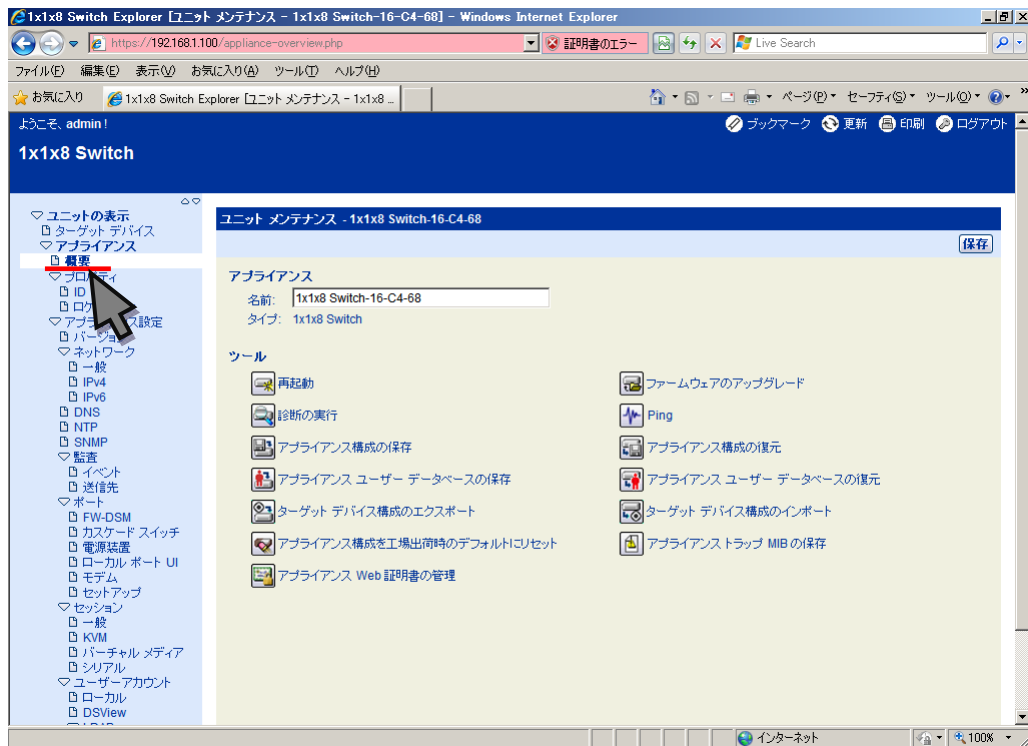
アプライアンス トラップ MIB の保存 - 1x1x8 Switch-16-C4-68
ダウンロード キャンセル
1x1x8 Switch-16-C4-68 のアプライアンス トラップ MIB ファイルを保存する場所を選択してください。
方式: ファイル システム TFTP FTP HTTP PUT
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ••••
MIB ファイル: ファイル名: TRAP-MIB.ASN

［保存先方式が ”HTTP” の場合］

”HTTP” は、HTTP サーバー上にファイルを保存する場合の方式です。
”HTTP” をラジオボタンで選択すると下のようなページが表示されます。HTTP サーバーのアドレス、HTTP サーバーへアクセスするユーザー名およびパスワード、保存ファイル名を入力し、［ダウンロード］ボタンをクリックします。

アプライアンス トラップ MIB の保存 - 1x1x8 Switch-16-C4-68
ダウンロード キャンセル
1x1x8 Switch-16-C4-68 のアプライアンス トラップ MIB ファイルを保存する場所を選択してください。
方式: ファイル システム TFTP FTP HTTP PUT
サーバー: 192.168.1.50
ユーザー名: test
パスワード: ••••
MIB ファイル: ファイル名: TRAP-MIB.ASN

3.6.14 Web 証明書の管理

本装置に OBWI アクセスするための Web 証明書に関する設定を行うことができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると下のようなページが表示されます。[アプライアンス Web 証明書の管理]ボタンをクリックします。

下のようなページが表示されます。証明書の内容が表示されます。

3.6.15 Web サーバー証明書のインポート

HTTPS 証明書を変更する場合、「HTTP 証明書の管理」ページにおいて、[更新]ボタンをクリックします。

下のようなページが表示されます。"自己署名の新しい証明書の生成" ラジオボタンを選択し、以下のテキストボックスに入力します。
"共通名" テキストボックスには、本装置の IP アドレスを入力します。入力後、右上の[生成]ボタンをクリックします。

HTTPS 証明書の管理 - 1x1x8 Switch-16-C4-68

生成 キャンセル

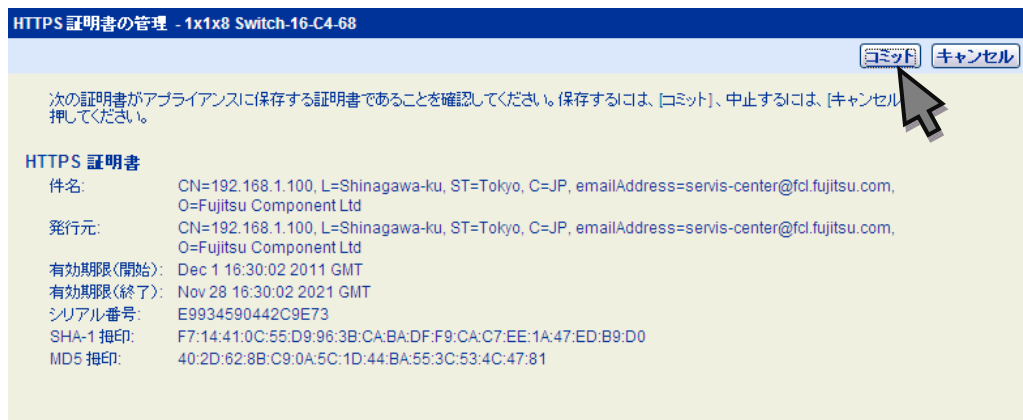
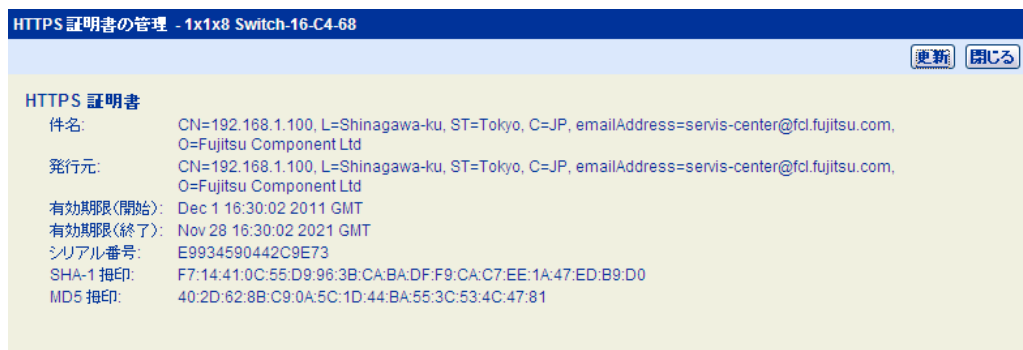
自己署名の新しい証明書を生成するか、証明書をアップロードするかを選択してください。アップロードされた証明書は、暗号化されていないプライベート キー付きの OpenSSL PEM 形式でなければなりません。

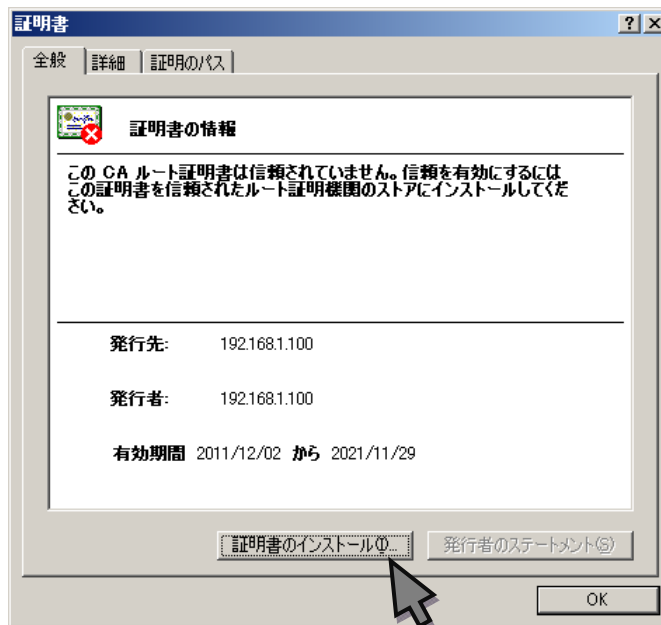
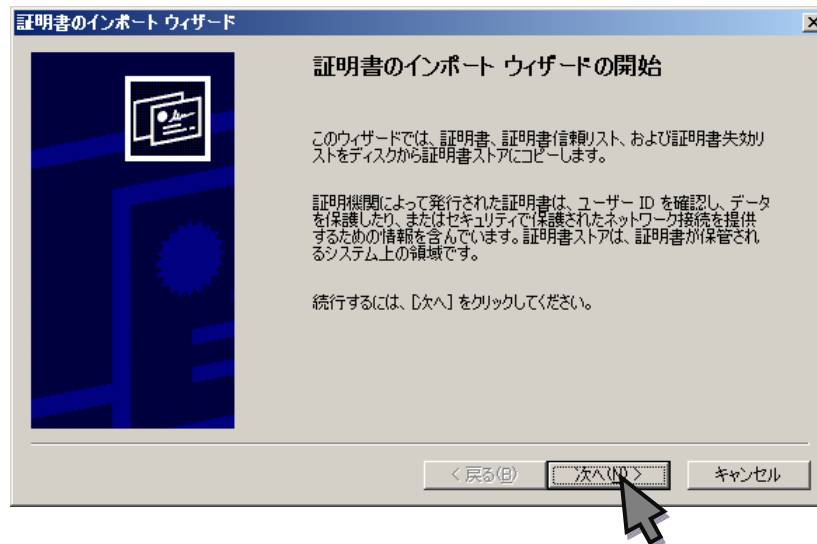
自己署名の新しい証明書の生成

共通名: 192.168.1.100
組織名: Fujitsu Component Ltd
市区町村または所在地: Shinagawa-ku
都道府県名: Tokyo
国名: JP
電子メール アドレス: servis-center@fcl.fujitsu.com

新しい証明書のアップロード

方式: ファイル システム TFTP FTP HTTP
OpenSSL PEM: ファイル名: 参照...

下のように、変更した証明書の内容が表示されます。保存する場合は、右上の[コミット]ボタンをクリックします。

変更が適用され、現在の HTTPS 証明書の表示に戻ります。

ブラウザのツールバーの上方に表示された「証明書のエラー」をクリックし、さらに表示されるポップアップ内の ”証明書の表示” をクリックします。

「証明書」ウィンドウが表示されます。"全般" タブで[証明書のインストール]ボタンをクリックします。

「証明書のインポートウィザード」ダイアログが表示されます。[次へ]ボタンをクリックします。

「証明書ストア」画面が表示されます。"証明書の種類に基づいて、自動的に証明書ストアを選択する" ラジオボタンを選択し、[次へ]ボタンをクリックします。

証明書のインポート ウィザード

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

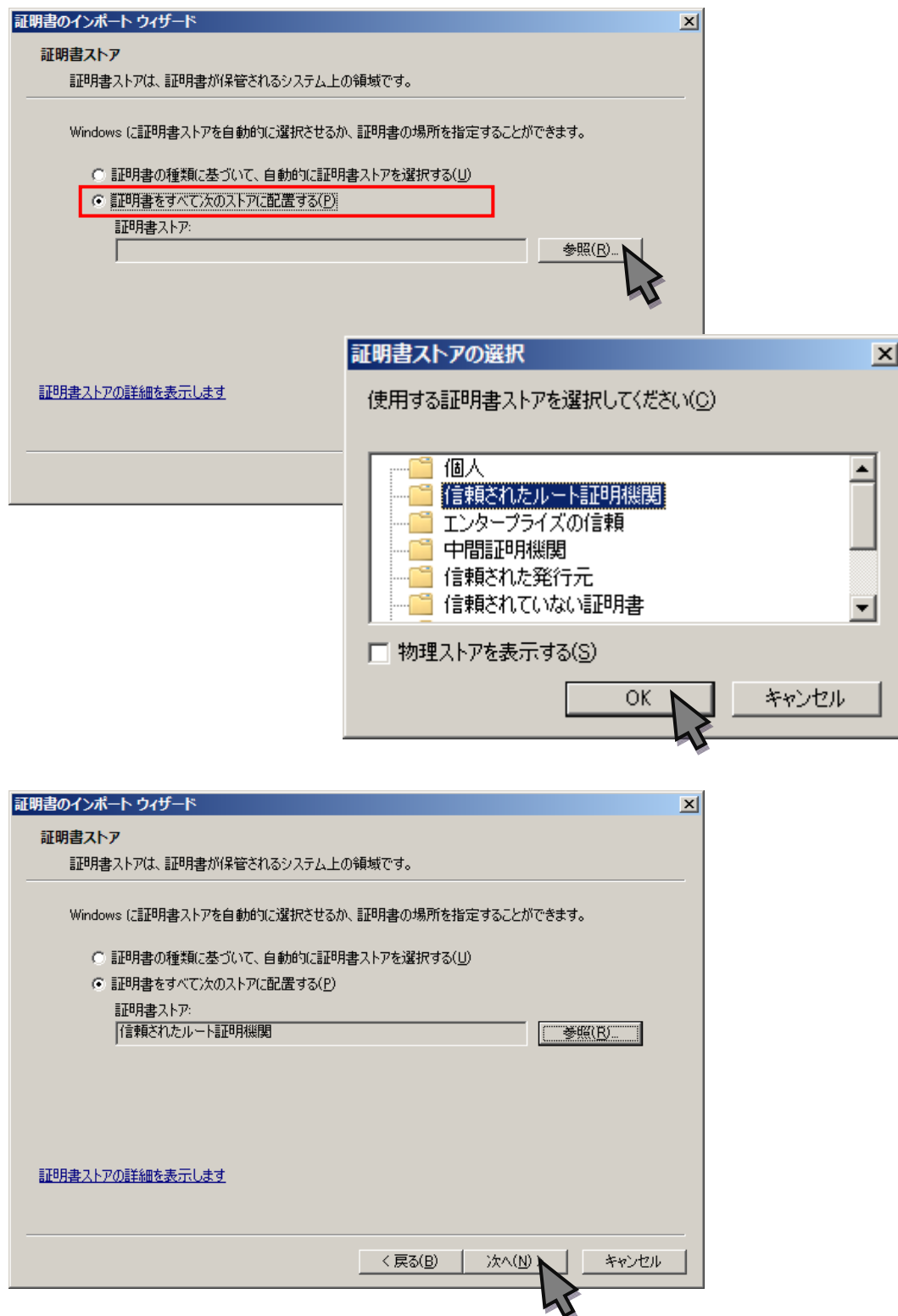
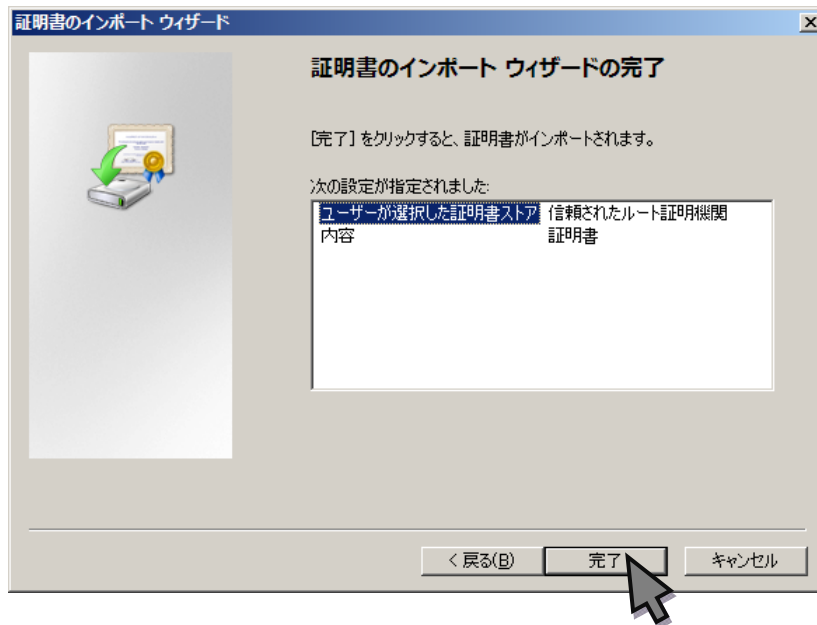
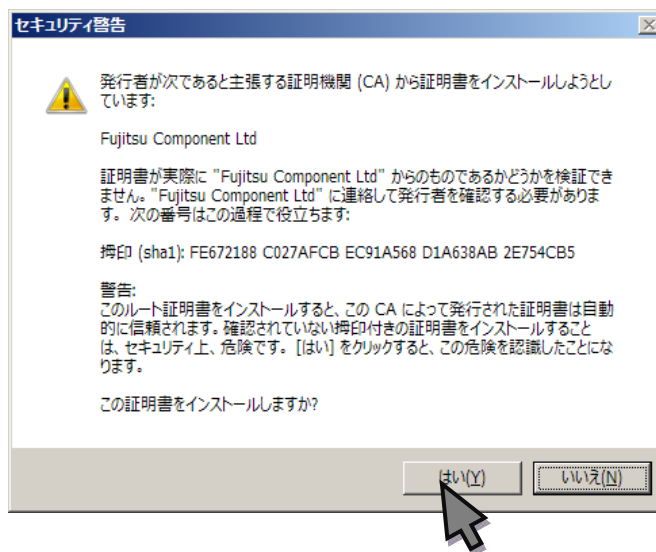
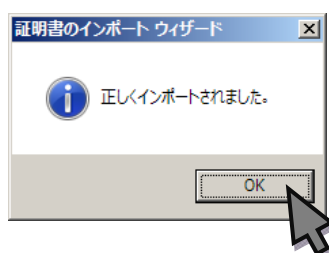
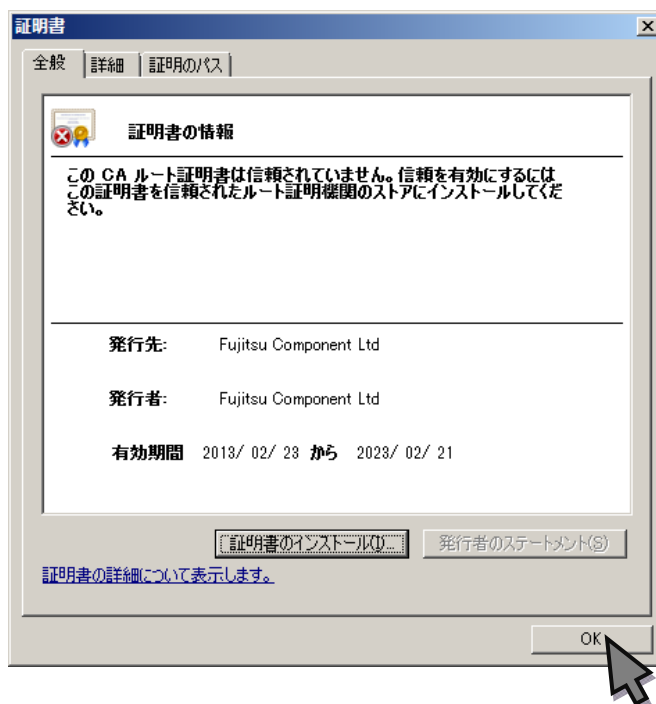
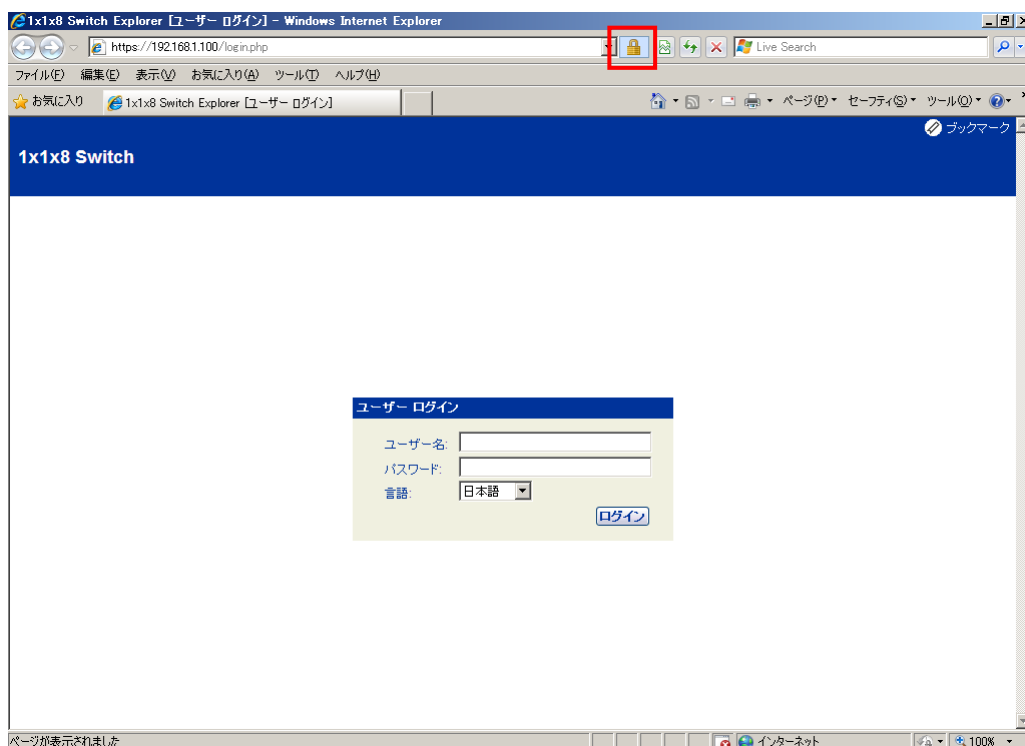
証明書をすべて次のストアに配置する(P)

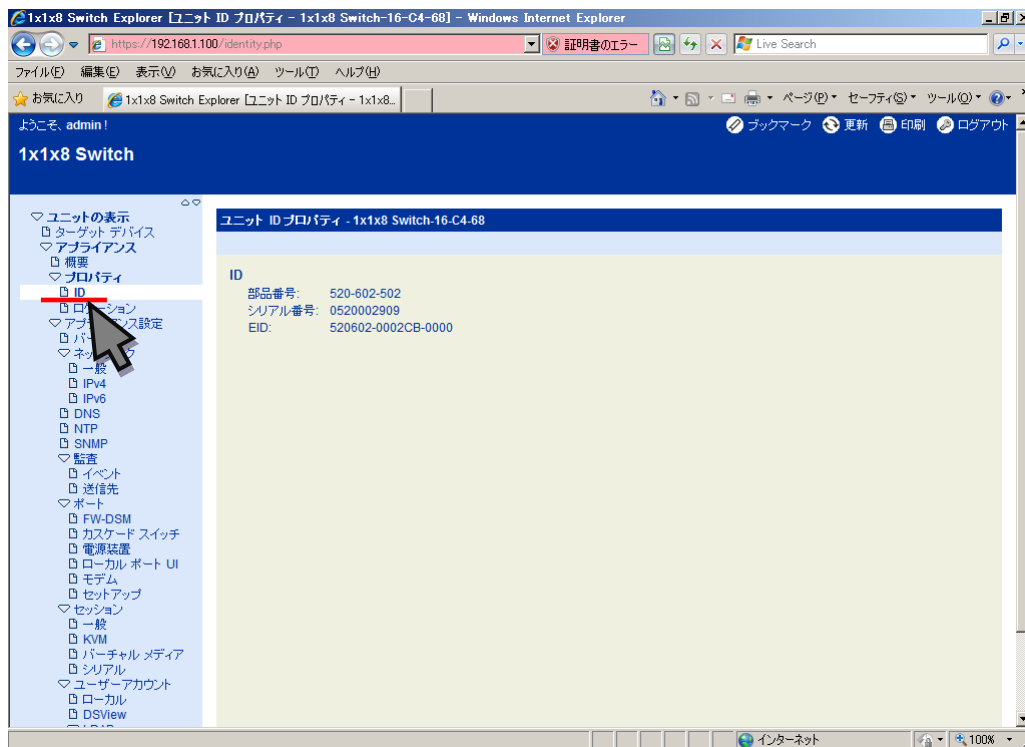
証明書ストア:

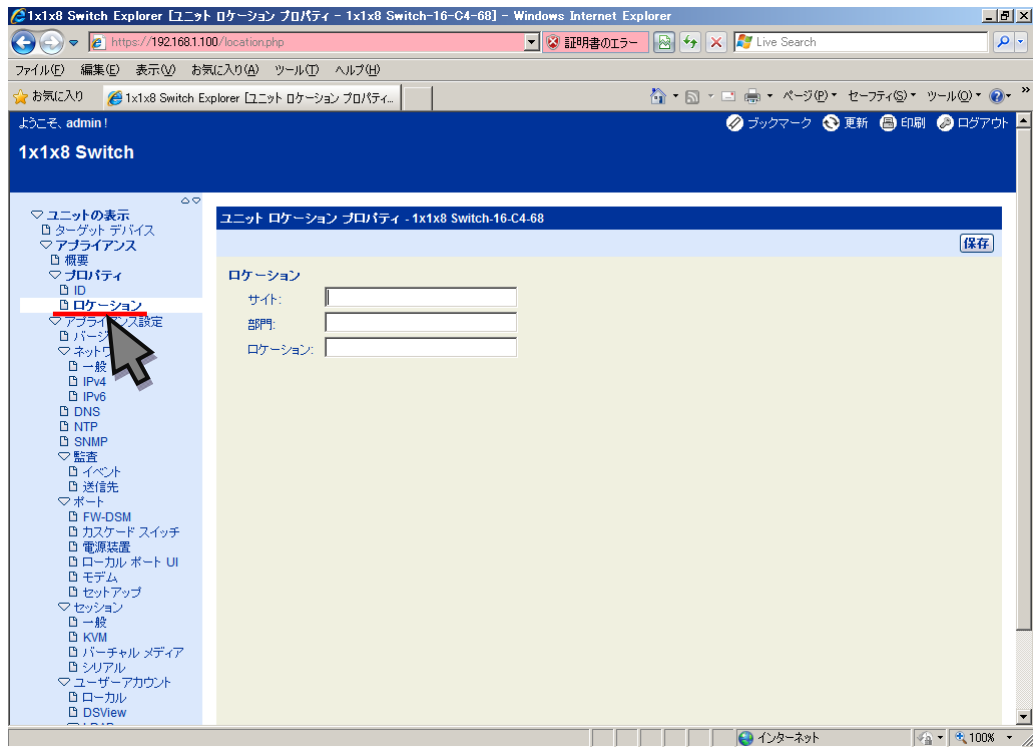
信頼されたルート証明機関

参照(R)...

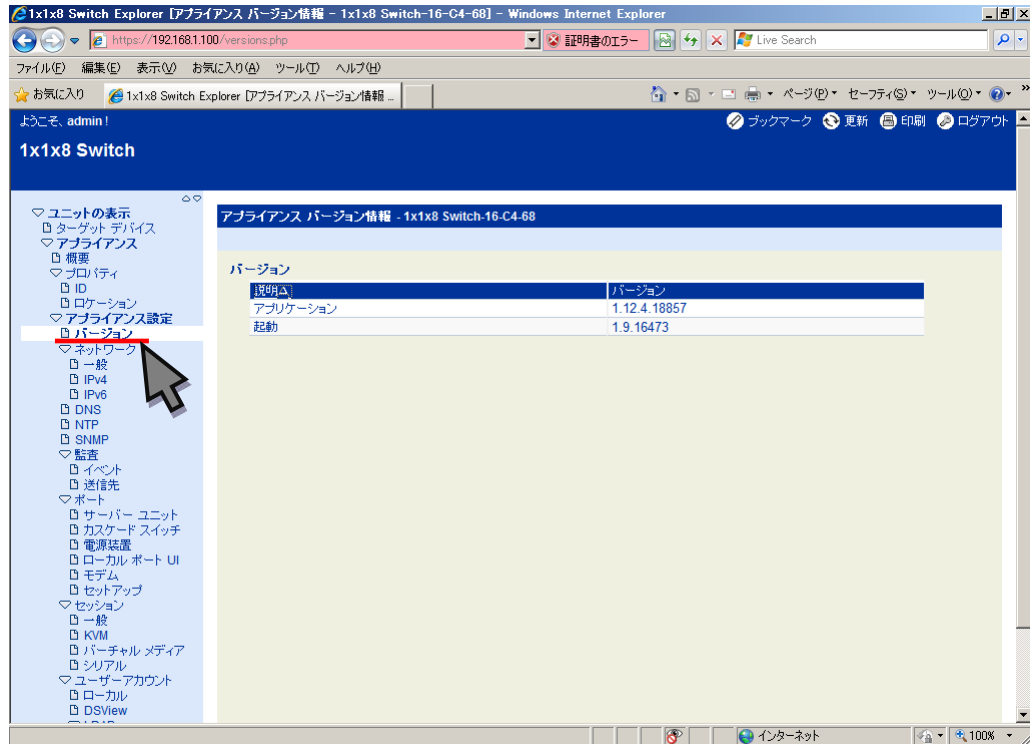
証明書ストアの詳細を表示します

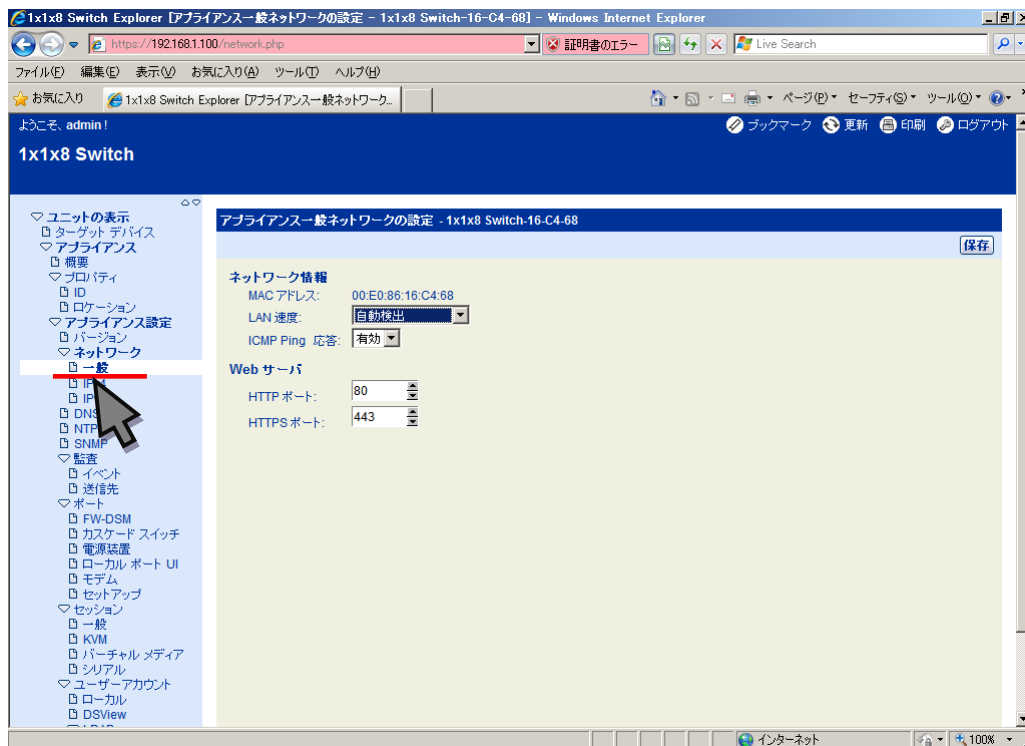
< 戻る(B)　次へ(N) >　キャンセル

下のように表示され、証明書のインポートウィザードが完了します。[完了]ボタンをクリックします。

セキュリティ警告のメッセージボックスが表示されます。証明書のインストールを実行するので、[はい]ボタンをクリックします。

下のようなメッセージが表示されれば、証明書のインポートは完了です。[OK]ボタンをクリックします。

「証明書」ウィンドウを閉じます。

<u>ブラウザを一度閉じて再度ブラウザを起動するか、新しいセッションを開始(Ctrl+N キー操作)</u>して、改めてログインページを開くと、下図のように証明書エラーは表示されなくなります。

3.7. ID 表示

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「プロパティ」-「ID」をクリックすると「ユニット ID プロパティ」ページが表示されます。本装置のシリアル番号、EID などを確認することができます。

3.8. ロケーション設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「プロパティ」-「ロケーション」をクリックすると「ユニット ロケーションプロパティ」ページが表示されます。本装置のサイト、部門、ロケーションを装置情報として設定することができます。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

3.9. バージョンの確認

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「バージョン」をクリックすると「アプライアンス バージョン情報」ページが表示されます。本装置のファームウェアバージョンを確認することができます。

3.10. 一般ネットワークの設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ネットワーク」-「一般」をクリックすると「アプライアンス 一般ネットワークの設定」ページが表示されます。本装置の MAC アドレスの確認、LAN 速度、Ping 応答の有効/無効、TCP ポート番号などの設定を行うことができます。

各設定項目は、ドロップダウンリストからの選択、あるいはスピンボタンによる値の指定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

アプライアンス一般ネットワークの設定 - 1x1x8 Switch-16-C4-68

保存

ネットワーク情報

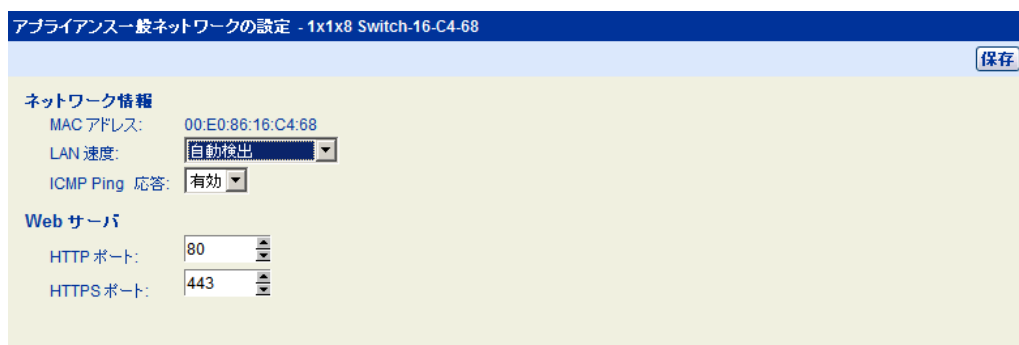
MAC アドレス: 00:E0:86:16:C4:68

LAN 速度: 自動検出

ICMP Ping 応答: 有効

Web サーバ

HTTP ポート: 80

HTTPS ポート: 443

設定詳細は、下記のとおりです。

項	表示項目	内容
ネットワーク情報		
1	LAN 速度	イーサネットモードを以下の設定から選択します。 "自動検出" : オートネゴシエーション動作 "10Mbps 半二重" : 10Mpbs, half duplex 固定 "10Mbps 全二重" : 10Mbps, full duplex 固定 "100Mbps 半二重" : 100Mpbs, half duplex 固定 "100Mbps 全二重" : 100Mpbs, full duplex 固定 "1Gbps 全二重" : 1Gpbs, full duplex 固定 デフォルトは、"自動検出" に設定されています。
2	ICMP Ping 応答	ICMP Ping に対する応答の有効/無効を指定します。 "無効" に設定すると本装置は Ping に応答しません。 デフォルトは、"有効" に設定されています。
Web サーバ		
3	HTTP ポート	HTTP プロトコルの TCP ポート番号を指定します。 デフォルトは、"80" に設定されています。
4	HTTPS ポート	HTTPS プロトコルの TCP ポート番号を指定します。 デフォルトは、"443" に設定されています。

LAN 速度を変更した場合は、本装置を再起動する必要があります。

参照 3.6.2 アプライアンスの再起動（50 ページ）

3.11. IPv4 の設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ネットワーク」-「IPv4」をクリックすると「アプライアンス IPv4 設定」ページが表示されます。本装置の IPv4 に関する設定を行うことができます。

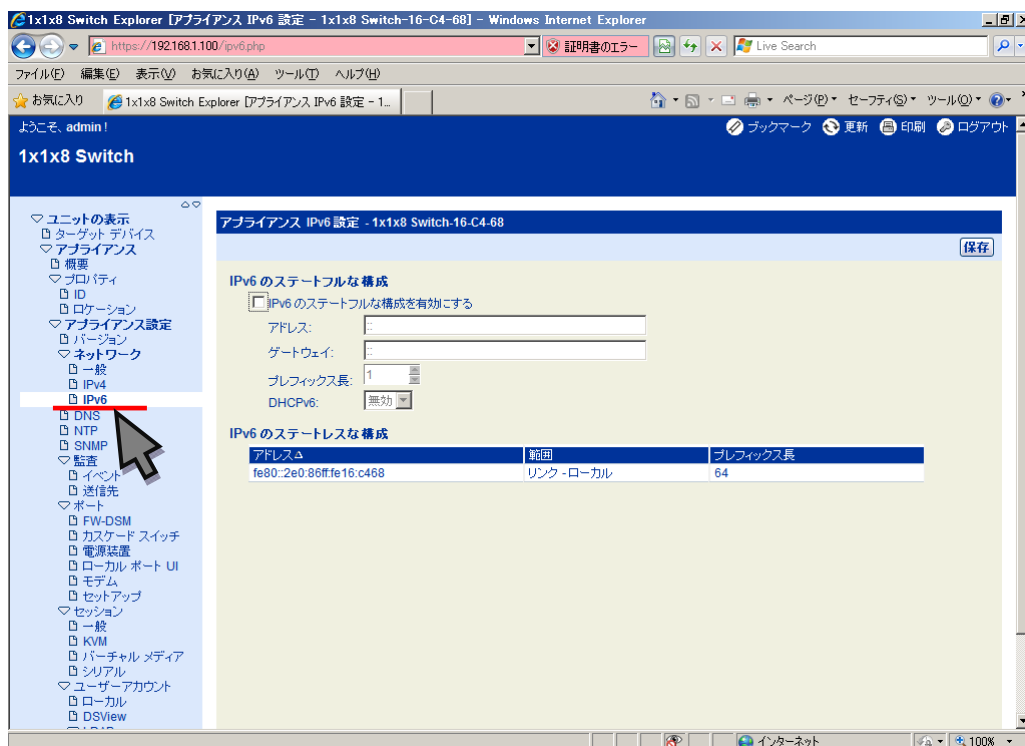
設定詳細は、下記のとおりです。

項	表示項目	内容
1	"IPv4 を有効にする" チェックボックス	本チェックボックスにチェックを入れると以下の項目がアクティブ表示になり、IPv4 に関する設定が有効となります。 チェックを外すと、以下の項目はグレイアウト表示となります。
2	アドレス	IPv4 のアドレスを指定します。
3	サブネット	IPv4 のサブネットマスクを指定します。
4	ゲートウェイ	IPv4 のデフォルトゲートウェイを指定します。
5	DHCP	DHCP の有効/無効を選択します。 "有効" を選択すると上記「アドレス」、「サブネット」、「ゲートウェイ」の設定テキストボックスがグレイアウト表示となります。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

「DHCP」を "有効" に設定すると、「アドレス」、「サブネット」、「ゲートウェイ」に設定されている各値は、無視されます。

3.12. IPv6 の設定

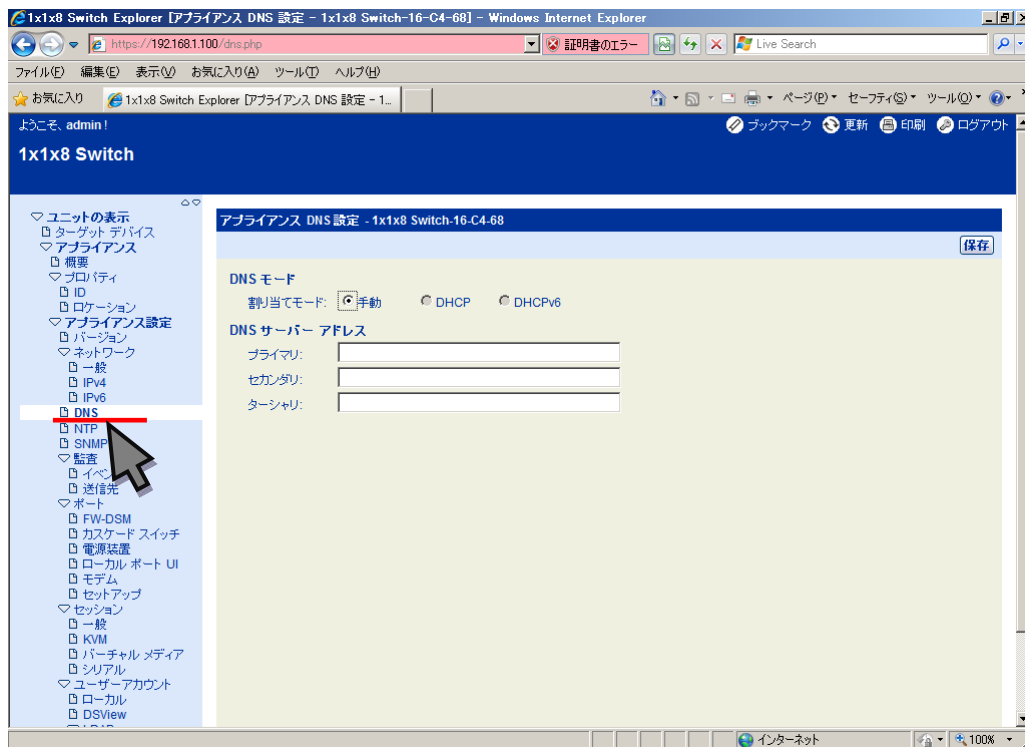
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ネットワーク」-「IPv6」をクリックすると「アプライアンス IPv6 設定」ページが表示されます。本装置の IPv6 に関する設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
1	"IPv6 のステートフルな構成を有効にする" チェックボックス	本チェックボックスにチェックを入れると以下の項目がアクティブ表示になり、IPv4 に関する設定が有効となります。 チェックを外すと、以下の項目はグレイアウト表示となります。
2	アドレス	IPv6 のアドレスを指定します。
3	ゲートウェイ	IPv6 のデフォルトゲートウェイを指定します。
4	プレフィックス長	1～128 の範囲でプレフィックス長を指定します。
5	DHCPv6	DHCP の有効/無効を選択します。 "有効" を選択すると上記「アドレス」、「ゲートウェイ」、「プレフィックス長」の設定テキストボックスがグレイアウト表示となります。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

「DHCPv6」を "有効" に設定すると、「アドレス」、「ゲートウェイ」、「プレフィックス長」に設定されている各値は、無視されます。

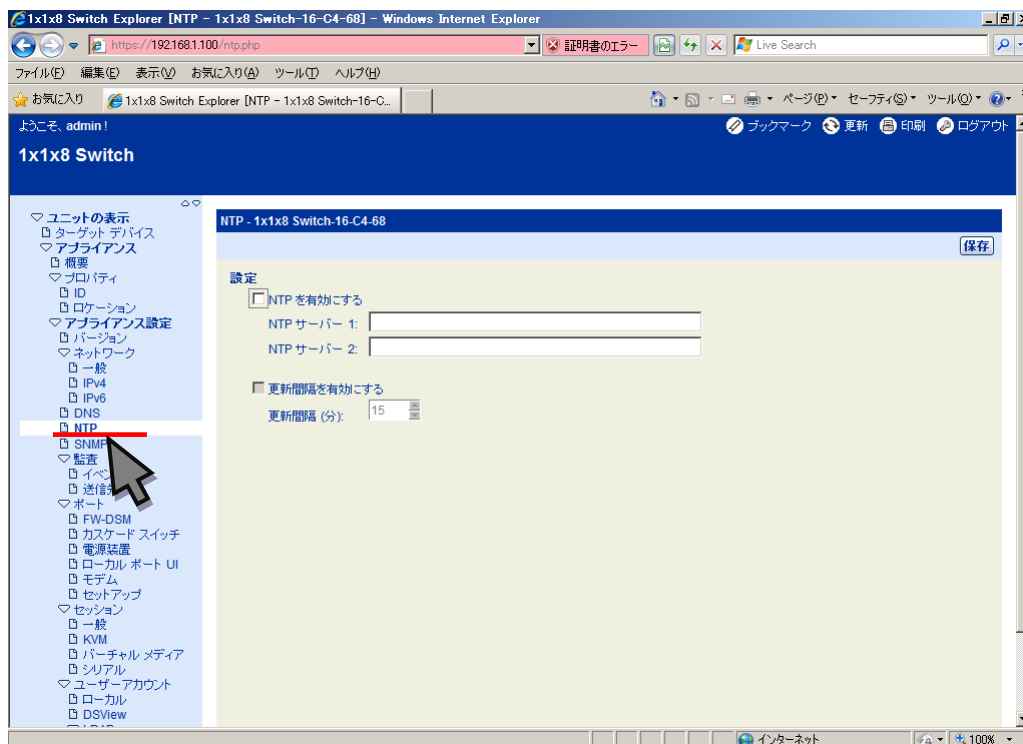
3.13. DNS の設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「DNS」をクリックすると「アプライアンス DNS 設定」ページが表示されます。本装置の DNS に関する設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
DNS モード		
1	割り当てモード	DNS の割り当てモードを選択します。 "手動"、"DHCP"、"DHCPv6" のいずれかを選択します。 IP アドレス設定において、DHCP が無効になっている場合、"DHCP" および "DHCPv6" は、グレイアウト状態となります。
DNS サーバーアドレス		
2	プライマリ	プライマリ DNS サーバーのアドレスを指定します。
3	セカンダリ	セカンダリ DNS サーバーのアドレスを指定します。
4	ターシャリ	ターシャリ DNS サーバーのアドレスを指定します。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

3.14. NTP の設定

本装置は、NTP サーバーと時刻同期させることができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「NTP」をクリックすると「NTP」ページが表示されます。本装置の NTP による時刻合わせに関する設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
1	"NTP を有効にする" チェックボックス	本チェックボックスにチェックを入れると NTP サーバーへの時刻調整が有効となります。
2	NTP サーバー1	NTP サーバー1 台目のアドレスを指定します。
3	NTP サーバー2	NTP サーバー2 台目のアドレスを指定します。
4	"更新間隔を有効にする" チェックボックス	本チェックボックスにチェックを入れると一定の間隔で NTP サーバーへ時刻調整を実行します。
5	更新間隔(分)	時刻調整を行う間隔を 1～99(分単位)の範囲で指定します。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

3.15. SNMP の設定

本装置は、SNMP エージェント機能を持ち、本装置を管理するための情報を提供します。画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「SNMP」をクリックすると「SNMP」ページが表示されます。本装置の SNMP に関する設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
システム		
1	”SNMP を有効にする” チェックボックス	本チェックボックスにチェックを入れると SNMP 機能が有効となります。
2	名前	本項目の設定は、system.sysName の値として送信されます。本設定とアプライアンスの概要ページで設定できるアプライアンスの名前は、同一の設定値になります。どちらか一方を変更すると他方にも反映されます。
3	連絡先	本項目の設定は、system.sysContact の値として送信されます。
コミュニティ		
4	読み取り	読み取りコミュニティ名を指定します。
5	書き込み	書き込みコミュニティ名を指定します。
6	トラップ	トラップコミュニティ名を指定します。
許可管理マネージャー		
7	許可管理マネージャー 1～4	SNMP マネージャーの IP アドレスを指定します。 4 つまで指定することができます。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

3.16. イベントの設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「監査」-「イベント」をクリックすると「イベント」ページが表示されます。本装置の様々なイベントの通知機能に関する設定を行うことができます。

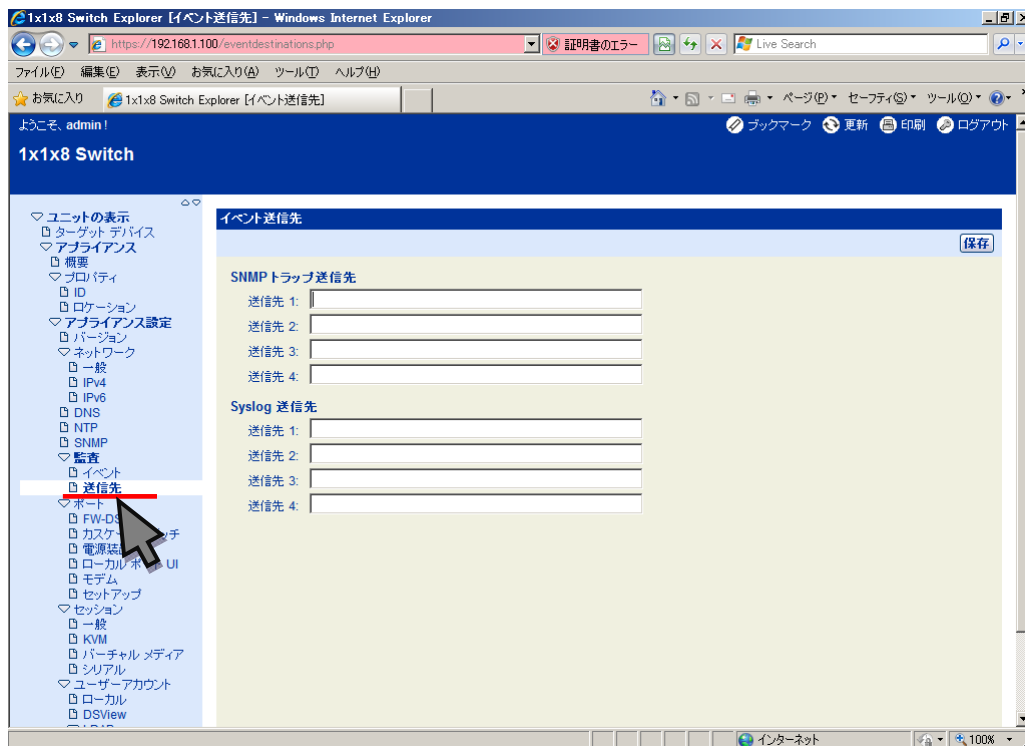
イベント発生時に通知するイベント内容を選択します。
任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

全てのイベントがデフォルトで選択された状態になっています。

本設定にて選択したイベントについて、SNMP マネージャーへのトラップ送信 あるいは Syslog サーバーSyslog 送信により、通知させることができます。送信先の設定については、下記をご参照ください。

📖 参照 3.17 イベント送信先の設定（104 ページ）

3.17. イベント送信先の設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「監査」-「送信先」をクリックすると「イベント送信先」ページが表示されます。本装置の任意のイベント発生時にSNMPトラップあるいはSyslogを送信する送信先の設定を行うことができます。

設定詳細は、下記のとおりです。

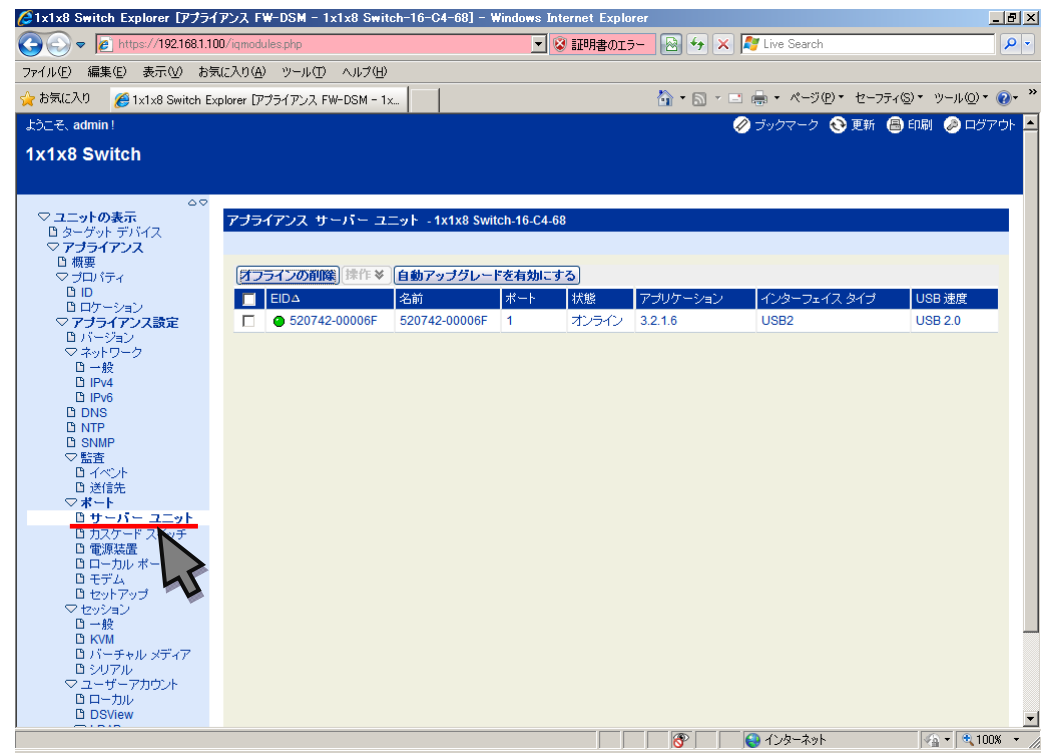
項	表示項目	内容
SNMP トラップ送信先		
1	送信先 1～4	SNMP トラップの送信先マネージャーの IP アドレスを指定します。4 つまで指定することができます。
Syslog 送信先		
2	送信先 1～4	Syslog 送信先の IP アドレスを指定します。 4 つまで指定することができます。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

通知するイベントの選択については、下記をご参照ください。

📖 参照 3.16 イベントの設定（103 ページ）

3.18. サーバーユニットの設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「サーバーユニット」をクリックすると「アプライアンス　サーバーユニット」ページが表示されます。本装置に接続されているサーバーユニットに関する設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
1	オフラインの削除	オフライン状態のサーバーユニットをリスト表示から削除します。 📖 参照 3.18.1 オフライン状態のサーバーユニットの表示クリア（107 ページ）
2	自動アップグレードを有効にする	サーバーユニットのファームウェアの自動アップグレードを有効にします。 📖 参照 3.18.4 サーバーユニットの自動アップグレード（110 ページ）

EID 項目に表示されるインジケーター表示により、以下の状態を示します。

表示	状態	説明
	オンライン	サーバーは電源が入っており、アクセス可能な状態です。
	オフライン	サーバーは電源オフあるいは、本装置とサーバーユニットが接続されていない状態です。
	アップグレード中	サーバーユニットのアップグレード中です。 ターゲットデバイスへのアクセスはできません。

操作対象のサーバーユニットがオンラインの状態において、左側に表示されているチェックボックスにチェックを入れると[操作]ボタンがアクティブ表示されます。
[操作]ボタンをクリックすると以下の操作が可能となります。

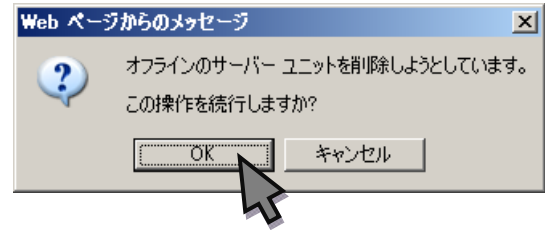
”USB1.1 速度にセット” および ”USB2.0 速度にセット” は、FW-DSM02/PS2-M および FW-DSM02/USB-L サーバーユニット でのみ設定可能な項目です。
FW-DSM03/VMC サーバーユニットでは設定することができません。

項	表示項目	内容
1	アップグレード	サーバーユニットのファームウェアをアップグレードします。 参照 3.18.3 サーバーユニットのアップグレード（109 ページ）
2	USB1.1 速度にセット	サーバーユニットの USB 速度を USB1.1 に設定します。 参照 3.18.5 サーバーユニットの USB 速度設定（111 ページ）
3	USB2.0 速度にセット	サーバーユニットの USB 速度を USB2.0 に設定します。 参照 3.18.5 サーバーユニットの USB 速度設定（111 ページ）
4	デフォルト設定の復元	サーバーユニットの設定をデフォルトの状態に戻します。

3.18.1 オフライン状態のサーバーユニットの表示クリア

サーバーユニットの一覧表示から、オフライン状態（ステータスが 赤色×表示になっている）のサーバーユニットの表示をクリアすることができます。

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「サーバーユニット」をクリックすると「アプライアンスサーバーユニット」ページが表示されます。下のように、[オフラインの削除]ボタンをクリックします。

下のような確認メッセージが表示されます。オフラインのサーバーユニットの表示をリストから削除する場合は、[OK]ボタンをクリックします。

オフライン状態のサーバーユニットが一覧表示から削除されます。
OBWI の全ての表示に反映されます。

3.18.2 サーバーユニットのバージョン確認

サーバーユニットのファームウェア バージョンを確認することができます。

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「サーバーユニット」をクリックすると「アプライアンス サーバーユニット」ページが表示されます。下のように、バージョンを確認するサーバーユニットの EID 番号をクリックします。

下のようなページが表示されます。サーバーユニットのバージョンなど各種情報を確認することができます。右上の[アップグレード]ボタンをクリックするとファームウェアのアップグレードが開始されます。

3.18.3 サーバーユニットのアップグレード

サーバーユニットのアップグレードを行うことができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「サーバーユニット」をクリックすると「アプライアンス サーバーユニット」ページが表示されます。

下のように、アップグレードを行うサーバーユニットのチェックボックスにチェックを入れ、「操作」メニューから ”アップグレード” をクリックします。

サーバーユニットのアップグレードを実行する場合、現在ターゲットデバイスへアクセスしているビューアのセッションは切断されます。

下のような確認メッセージが表示されます。アップグレードを実行する場合は、[OK]ボタンをクリックします。

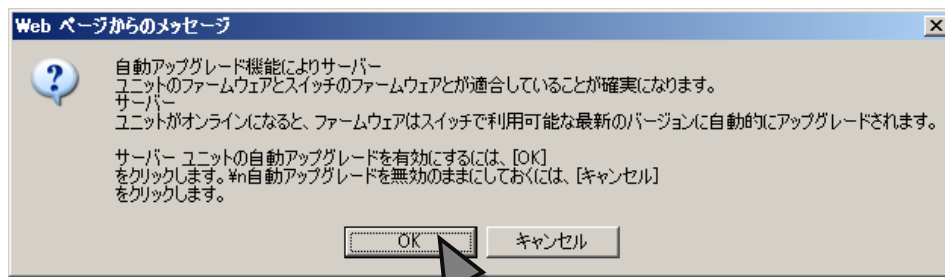
下のように表示され、アップグレードが開始されます。アップグレードの実行中は、「状態」項目に ”アップグレード中” と表示されます。サーバーユニットのアップグレード中は、ターゲットデバイスへの接続はできません。

アップグレードには、約 7 分かかります。「状態」項目の表示が ”オンライン” に戻れば、アップグレードは完了です。

3.18.4 サーバーユニットの自動アップグレード

サーバーユニットのファームウェアのバージョンを認識して、必要であれば自動的にアップグレードを行うように設定することができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「サーバーユニット」をクリックすると「アプライアンス サーバーユニット」ページが表示されます。

下のように、[自動アップグレードを有効にする]ボタンをクリックします。

下のような確認メッセージが表示されます。自動アップグレード機能を有効にする場合は、[OK]ボタンをクリックします。

自動アップグレード機能が有効になります。

これにより、本装置に接続されているサーバーユニットがオンラインの状態になり、現在のファームウェアからアップグレードが可能な状態の場合には自動的にアップグレードが実行されます。
自動アップグレード機能を無効にする場合は、[自動アップグレードを無効にする]ボタンをクリックします。

重要

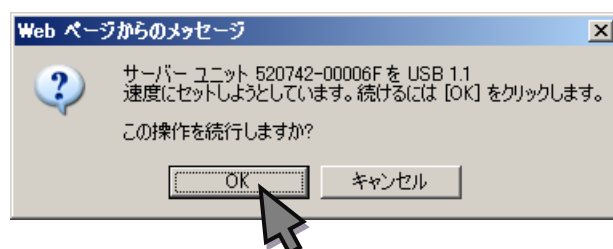
本製品は初期状態で **サーバーユニットの自動アップグレードが有効** になっております。アップグレード時間はサーバーユニット毎に約 7 分かかりますが、その間、**本体側の電源を切らないようお願い致します。**自動アップグレードの対象は DSM02 シリーズのサーバユニットとなります。本製品に取り付けの際は予めご了承ください。

参照 3.18.3 サーバーユニットのアップグレード（109 ページ）

3.18.5 サーバーユニットの USB 速度設定

FW-DSM02/PS2-M および FW-DSM02/USB-L サーバーユニットの USB 速度を設定することができます。USB1.1 あるいは USB2.0 を選択します。ターゲットデバイスの OS が正常に起動しない場合などには、USB1.1 に設定することにより、改善されることがあります。
なお、本設定は、FW-DSM03/VMC サーバーユニットでは設定することができません。

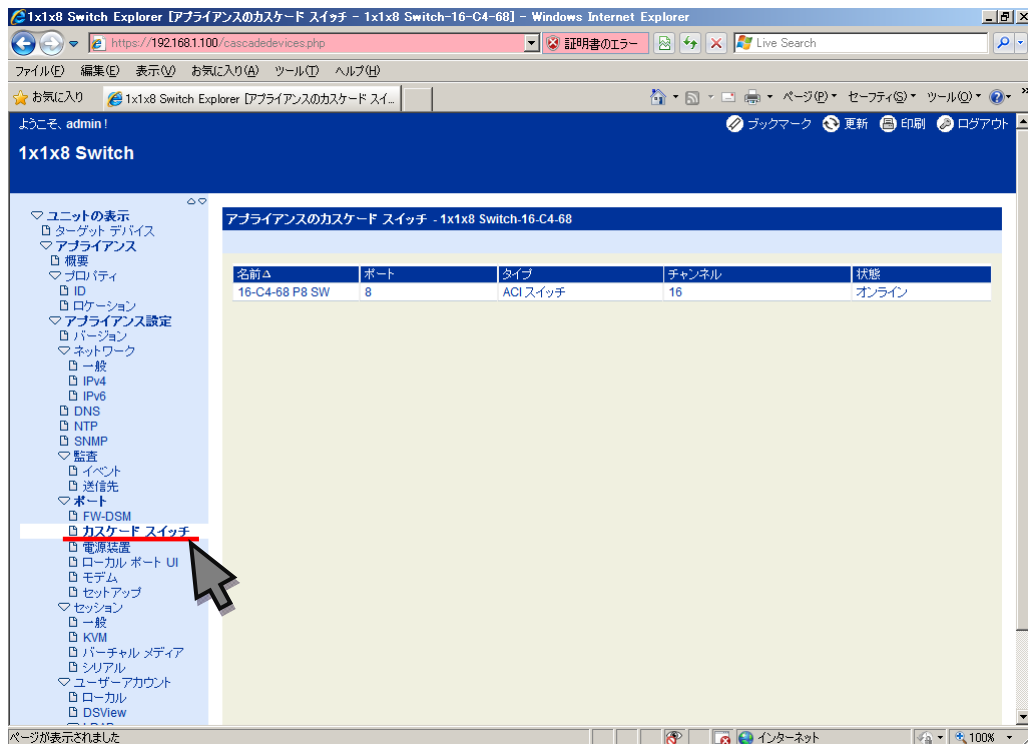
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「サーバーユニット」をクリックすると「アプライアンス サーバーユニット」ページが表示されます。下のように、USB 速度設定を行う サーバーユニットのチェックボックスにチェックを入れ、「操作」メニューから ”USB1.1 速度にセット” あるいは ”USB2.0 速度にセット” をクリックします。（下の例では、USB1.1 に設定しています。）

下のような確認メッセージが表示されます。USB 速度の変更を実行する場合は、[OK]ボタンをクリックします。

USB 速度の変更が実行されます。下のように、「USB 速度」項目の表示で現在の設定を確認することができます。

3.19. カスケード接続の状態確認

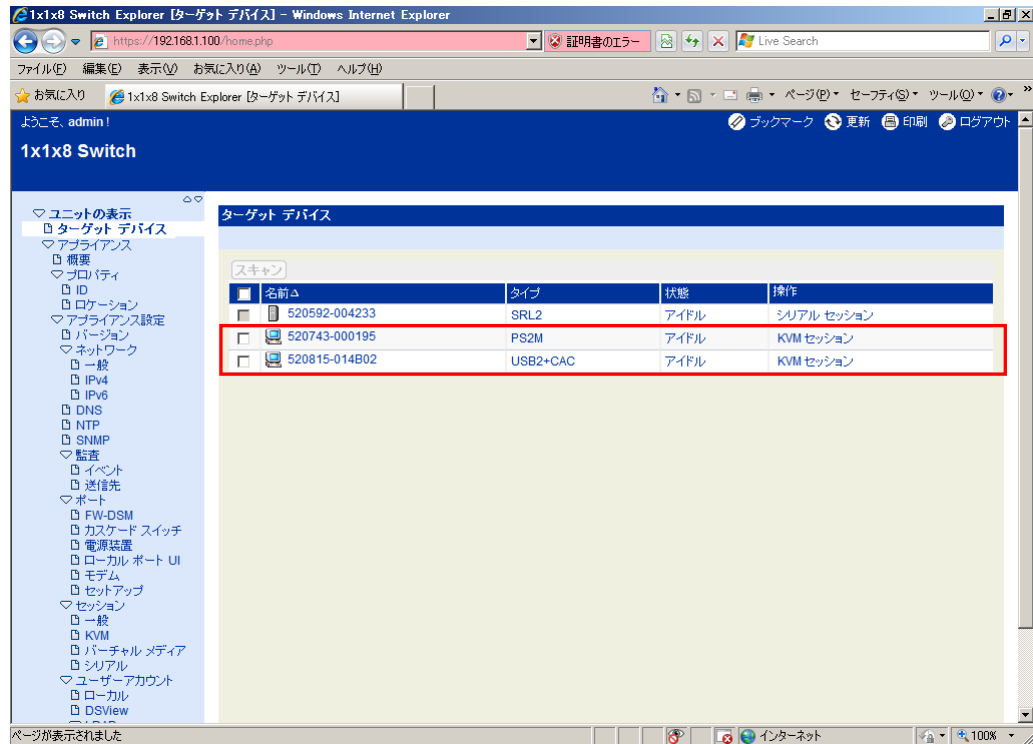
本製品は、装置本体を 2 段までカスケード接続することができます。

📖 参照 1.6 カスケード接続（12 ページ）

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「カスケードスイッチ」をクリックすると「アプライアンスのカスケードスイッチ」ページが表示されます。本装置のカスケード接続に関する状態を確認することができます。

本装置がカスケード接続により、マスター装置側になっている場合、スレーブ装置の情報が下のように表示されます。

各項目の表示内容は下のとおりです。

項	表示項目	内容
1	名前	スレーブ側装置の名称を示します。
2	ポート	カスケード接続を行っている、マスター装置側のターゲットポート番号を示します。
3	タイプ	スレーブ装置のタイプを示します。 "ACI スイッチ" と表示されます。
4	チャンネル	スレーブ装置側のターゲットポート数を示します。
5	状態	スレーブ装置の動作状態を示します。 電源投入状態の場合、"オンライン" と表示されます。 電源オフ状態の場合、"オフライン" と表示されます。

カスケード接続している場合、マスター装置側のターゲットデバイス一覧に、スレーブ装置に接続されているターゲットデバイスの情報も合わせて表示されます。
下の赤枠内は、スレーブ側に接続されたターゲットデバイスです。特別にスレーブ側のターゲットデバイスであることを意識することなく操作することができます。

スレーブ装置に接続されたターゲットデバイスへのアクセスにつきましては、操作項目の ”KVM セッション” あるいは ”シリアルセッション” をクリックします。

これにより、ビューア画面が起動し、スレーブ側のターゲットデバイスの操作を実行することができます。
ビューア画面の操作方法については、カスケード接続することなく単独で本製品をお使いいただいている場合と同様です。

3.20. 電源装置の設定

本製品は、オプションの電源装置と接続し、組み合わせてご利用いただくことにより、ターゲットデバイスの電源制御（ON/OFF 操作）を行うことができます。

参照 1.8 電源装置との接続（14 ページ）

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「電源装置」をクリックすると「アプライアンス電源装置」ページが表示されます。本装置と電源装置を組み合わせて使用する場合の設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
1	オフラインの削除	オフライン状態の電源装置をリスト表示から削除します。
2	アウトレットへのデフォルト名の割り当て	アウトレット名称にデフォルト名を設定します。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

3.20.1 電源装置の詳細設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「電源装置」をクリックすると「アプライアンス電源装置」ページが表示されます。
本装置の PDU ポートに電源装置が接続されており、本装置に認識されると、下のように表示されます。電源装置の名称をクリックします。

下のようなページが表示されます。

設定内容詳細は、下のとおりです。

項	表示項目	内容
1	名前	電源装置の名称を指定します。
2	説明	電源装置に関する説明を記入することができます。
3	ブザー	電流値がしきい値を超えた場合のアラーム音の有効/無効を設定します。
4	過電流保護	過電流保護機能の有効/無効を設定します。 過電流保護機能が有効になっていると電源装置全体で消費

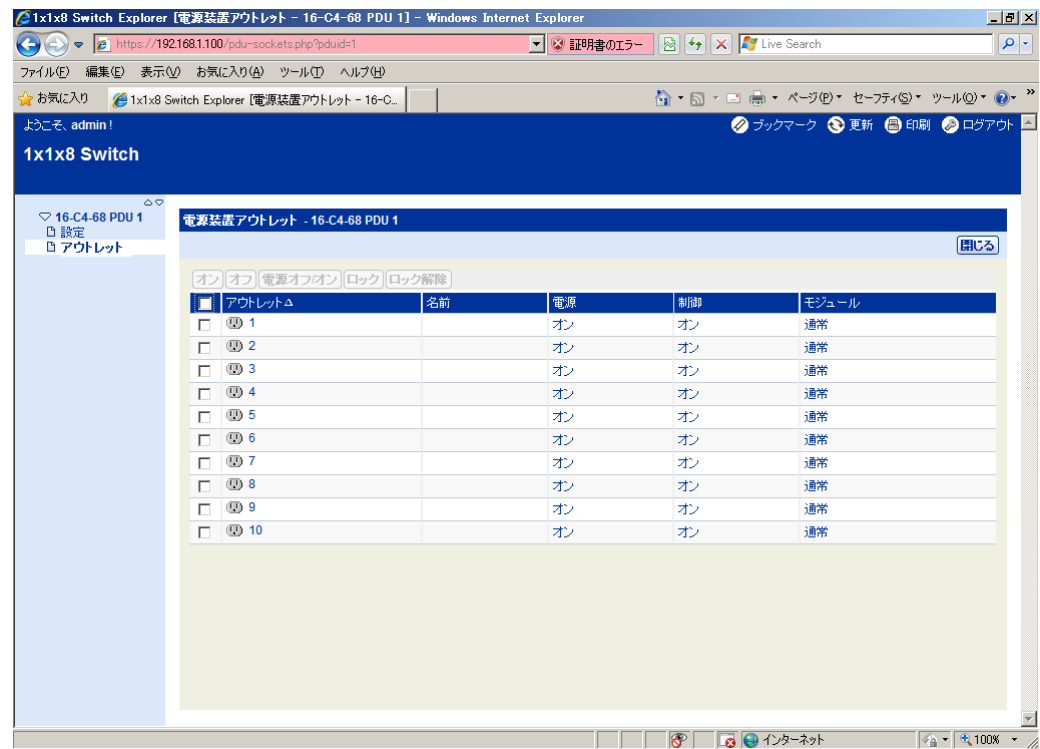
		される電流値がアラームのしきい値を超えた場合にコンセントがオンにならないようにすることができます。
5	アラームのしきい値	ブザー通知における、消費電流のしきい値を設定します。 2～15（A 単位）の範囲で指定することができます。
6	電源オフ/オンの遅延	電源装置のコンセントをオフにしてからオンにする動作において、オフからオンするまでの待ち時間を設定します。 1～60（秒単位）の範囲で指定することができます。
7	ファームウェアのアップグレード	電源装置のファームウェアをアップグレードすることができます。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

3.20.2 アウトレットの設定

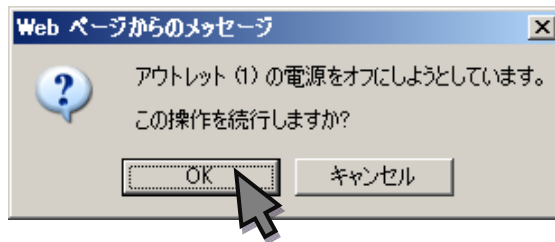
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「電源装置」をクリックすると「アプライアンス電源装置」ページが表示されます。電源装置の名称をクリックします。

下のようなページが表示されます。画面左のメニュー選択領域で「アウトレット」をクリックします。

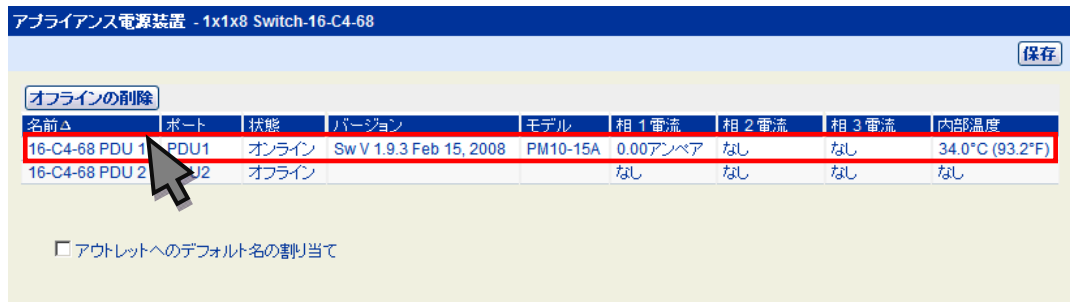
下のような、「電源装置アウトレット」ページが表示されます。

設定内容詳細は、下のとおりです。

項	表示項目	内容
1	オン	選択したアウトレットの電源をオンします。
2	オフ	選択したアウトレットの電源をオフします。
3	電源オフ/オン	選択したアウトレットの電源をオフし、一定時間の後、オンします。
4	ロック	選択したアウトレットのオン/オフ操作ができないようにロックします。
5	ロック解除	選択したアウトレットのロックを解除します。

アウトレットを操作する場合は、任意のアウトレットのチェックボックスにチェックを入れ、操作ボタンをクリックします。下の例では、アウトレット 1 をオフにします。

下のような確認メッセージが表示されます。操作を実行する場合は、[OK]ボタンをクリックします。

アウトレット操作が実行され、しばらくするとアウトレット状態がリスト一覧に反映されます。
下の例では、アウトレット 1 がオフ状態であることが確認できます。

3.20.3 電源アウトレットの関連付け

電源装置のアウトレットとサーバーユニットを関連付けることができます。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「電源装置」をクリックすると「アプライアンス電源装置」ページが表示されます。電源装置の名称をクリックします。

下のようなページが表示されます。画面左のメニュー選択領域で「アウトレット」をクリックします。

下のようなページが表示されます。設定を行うアウトレットのアイコンをクリックします。下の例では、アウトレット 1 を選択しています。

下のような「電源装置アウトレットの設定」ページが表示されます。

設定内容詳細は、下のとおりです。

項	表示項目	内容
1	手動	本設定を選択すると「ターゲットデバイス」ページのリストにアウトレットが追加され、操作が可能となります。
2	名前	「ターゲットデバイス」ページに表示するアウトレットの名称を設定します。
3	ターゲットデバイスとのリンク	本設定を選択すると「ターゲットデバイス」ページに登録されているターゲットデバイスの ”操作” 項目にアウトレットの操作が追加されます。
4	ターゲットデバイス	アウトレットと関連付けるサーバーユニットをドロップダウンリストから選択します。
5	ターゲットデバイスとして表示しない	本設定を選択すると「ターゲットデバイス」ページのリスト上にはアウトレット情報を表示しません。
6	オン後の遅延時間	アウトレットのオンを実行してから、すぐにオフ操作させないようにするための遅延時間を設定します。0～100（秒単位）の範囲で指定することができます。

”手動” ラジオボタンを選択し、「名前」テキストボックスに登録するアウトレット名称を入力し、右上の[保存]ボタンをクリックします。

画面左のメニュー選択領域において、「ユニットの表示」-「ターゲットデバイス」をクリックすると「ターゲットデバイス」ページが表示されます。ターゲットデバイスのリストにアウトレットが追加されたのが確認できます。

アウトレットの操作を行う場合は、操作項目の ”⌄” をクリックし、任意の操作を選択します。

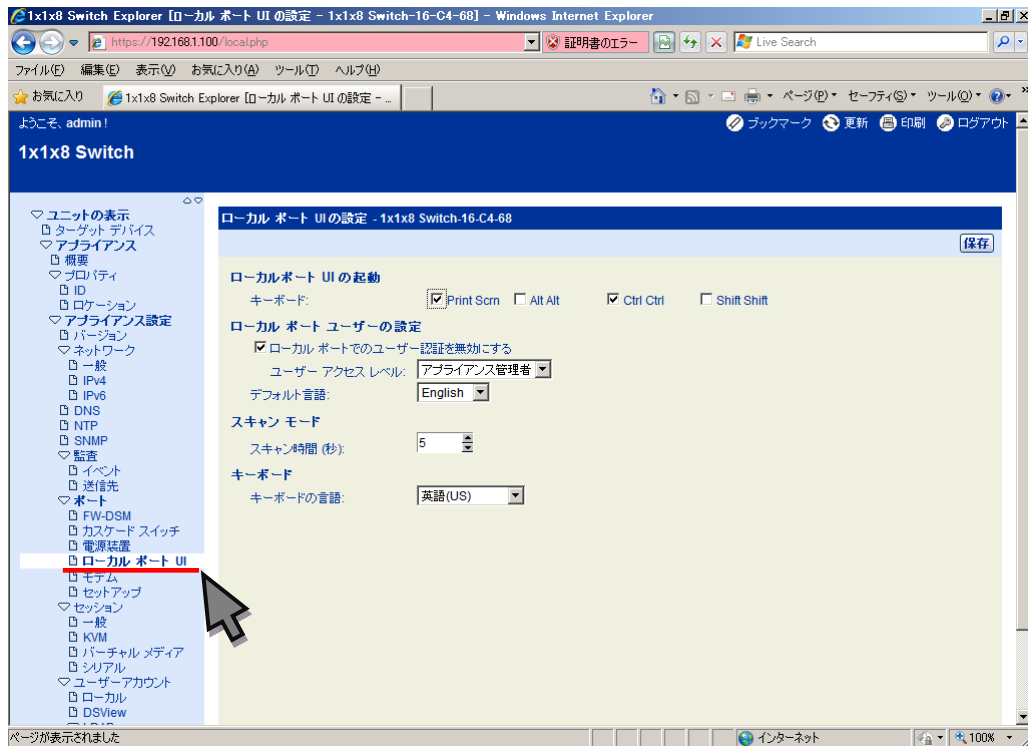
”壁電源オフ” を選択するとアウトレットの電源オフが実行されます。
”壁電源オフ/オン” を選択するとアウトレットの電源がオフされ、その後オンされます。

「電源装置アウトレットの設定」ページにおいて、"ターゲットデバイスとのリンク" ラジオボタンを選択し、「ターゲットデバイス」ドロップダウンリストから関連付けるサーバーユニットを選択して、右上の[保存]ボタンをクリックします。

画面左のメニュー選択領域において、「ユニットの表示」-「ターゲットデバイス」をクリックすると「ターゲットデバイス」ページが表示されます。ターゲットデバイスのリストにおいて、関連付けたターゲットデバイスのアウトレットの操作を行う場合は、操作項目の " " をクリックし、任意の操作を選択します。

"壁電源オフ" を選択するとアウトレットの電源オフが実行されます。
"壁電源オフ/オン" を選択するとアウトレットの電源がオフされ、その後オンされます。

3.21. ローカルポート UI の設定

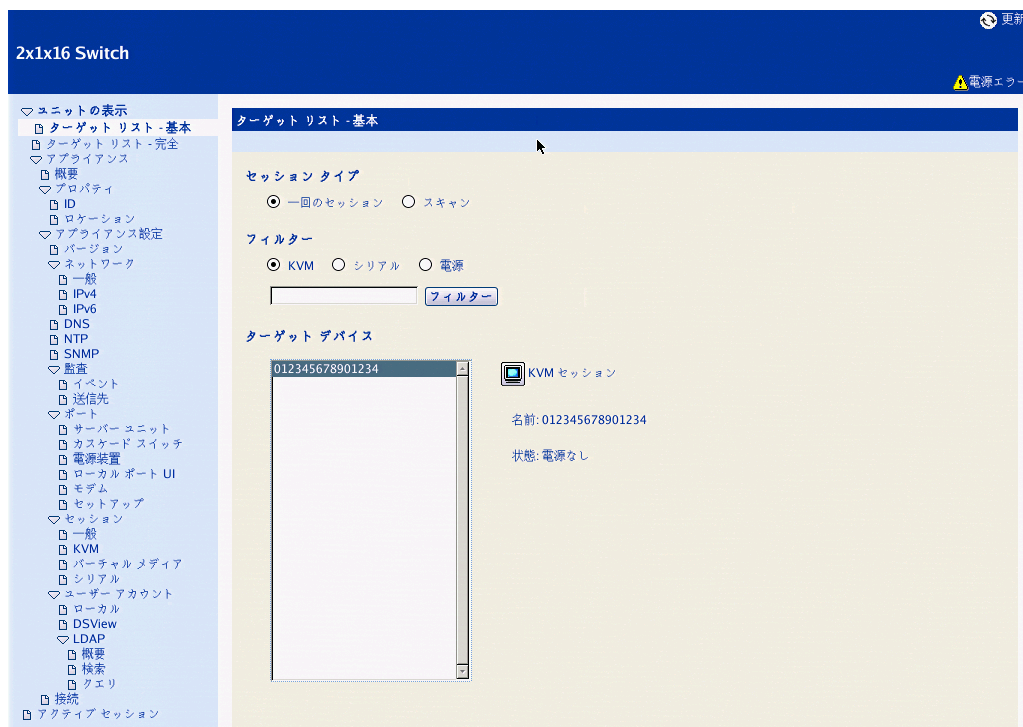
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「ローカルポート UI」をクリックすると「アプライアンス電源装置」ページが表示されます。本装置のローカルポート ユーザーインターフェース(ローカルポートUI)に関する設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
ローカルポート UI の起動		
1	キーボード	ローカルに接続したキーボードから、ローカルポート UI を表示するためのホットキーを下記の中から選択します。 ・PrintScrn : Print Screen キー1 回押下 ・Alt Alt : Alt キー2 回押下 ・Ctrl Ctrl : Ctrl キー2 回押下 ・Shift Shift : Shift キー2 回押下
ローカルポートユーザーの設定		
2	"ローカルポートでのユーザー認証を無効にする" チェックボックス	本チェックボックスのチェックを外すとローカル UI へのアクセスにおいて、ユーザー名とパスワードによるログイン認証が行われます。
3	ユーザーアクセスレベル	ローカルポートでのユーザー認証が無効の場合、ローカルユーザーのアクセスレベルを指定します。下記の中から選択します。 ・ユーザー ・ユーザー管理者 ・アプライアンス管理者 参照 3.29 ユーザーアクセスレベル (135 ページ)
4	デフォルト言語	ローカルポート UI の表示言語を指定します。
スキャンモード		

5	スキャン時間	ローカルポート UI において、スキャンモードを実行する場合の 1 台あたりのスキャン時間を指定します。3～255(秒単位)の範囲で指定することができます。
キーボード		
6	キーボードの言語	ローカルポートに接続したキーボードのキー配列言語をドロップダウンリストから選択します。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

重要:ローカルポートと OBWI の違い

ローカルポート UI では、ターゲットリストの表示方法で OBWI との違いを出しています。これは OBWI の応答よりもローカル UI の応答が少し遅いため、通常使われる機能をまとめたページを用意するべきだと考えた為です。
その為、ローカル UI のトップ画面は「ターゲットリスト – 基本」とし、下記の構成で表示する事にしています。

この画面以外は OBWI に合わせてあります。

また、OBWI では出来たスキャン機能を「ターゲットリスト – 基本」に設けています。
それぞれの機能は OBWI の相当機能となっておりますので、それぞれの説明は OBWI の各説明にて代替させて頂き、ここでの説明は割愛致します。

3.22. モデムの設定

V.34、V.90、V.92 のいずれかをサポートするモデム経由で本製品へアクセスすることができます。

📖 参照 1.7 モデム接続 (13 ページ)

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「モデム」をクリックすると「アプライアンスモデムの設定」ページが表示されます。本装置にモデム経由でアクセスする場合の設定およびアドレスの確認を行うことができます。

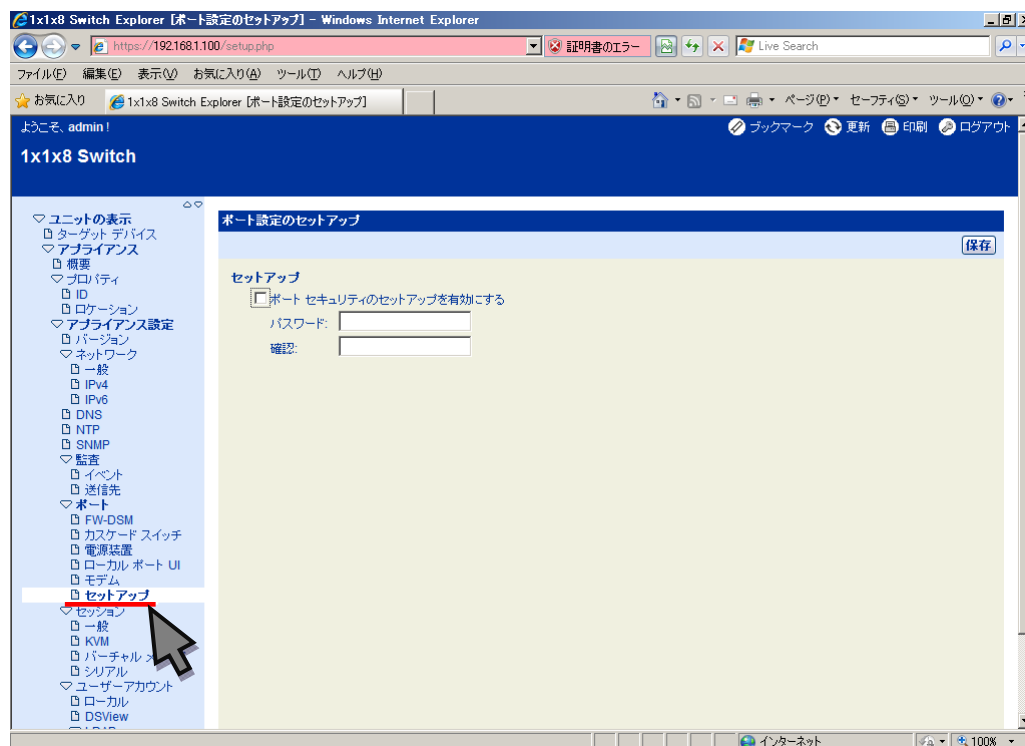
設定詳細は、下記のとおりです。

項	表示項目	内容
1	"モデムセッションではデジタルセッションを切断します" チェックボックス	本チェックを入れるとモデムセッションにおいて、ビデオセッションビューアを起動しようとすると、イーサネット経由でアクセスしていたセッションは切断されます。
2	認証タイムアウト(秒)	モデムセッションの認証タイムアウトを 30～300(秒)の範囲で指定します。
3	アイドルタイムアウト(分)	モデムセッションのアイドルタイムアウトを 1～60(分)の範囲で指定します。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

リモート端末からのモデム接続が確立すると、本装置のアドレスは 198.22.41.150、リモート端末のアドレスは 198.22.41.151 に設定されます。リモート端末から、198.22.41.150 のアドレスに対して、OBWI アクセスすることができます。

3.23. セットアップポートの設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「セットアップ」をクリックすると「ポート設定のセットアップ」ページが表示されます。本装置の SETUP ポートへシリアルコンソールアクセスする場合のセキュリティ設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
1	"ポート セキュリティのセットアップを有効にする" チェックボックス	本チェックボックスにチェックを入れると SETUP ポートからコンソールアクセスする場合のパスワード認証が有効になります。
2	パスワード	SETUP ポートからコンソールアクセスする場合のパスワードを入力します。
3	確認	SETUP ポートからコンソールアクセスする場合のパスワードを入力します(確認入力)。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

コンソールアクセス時の操作方法については、下記をご参照ください。

参照 5.7 ログインパスワードの入力 (238 ページ)

3.24. 一般セッションの設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「セッション」-「一般」をクリックすると「アプライアンス一般セッションの設定」ページが表示されます。OBWI やビデオセッションビューアのセッションに関する設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
アイドルタイムアウト		
1	”アイドルタイムアウトを有効にする” チェックボックス	セッションビューア画面のアイドルタイムアウトの有効/無効を指定します。本チェックボックスにチェックを入れると有効になります。
2	アイドルタイムアウト（分）	OBWI とセッションビューア画面のアイドルタイムアウト時間を指定します。1～90（分）の範囲で設定します。
ログインタイムアウト		
3	ログインタイムアウト（秒）	OBWII のログイン状態における、非アクティブ タイムアウト時間を指定します。20～120（秒）の範囲で設定します。
セッションタイムアウト		
4	”プリエンプトタイムアウトを有効にする” チェックボックス	ビデオセッションビューアにおいて、優先権のあるユーザーに接続を取られる際に通知ダイアログ表示を行うかの有効/無効を設定します。 本チェックボックスにチェックを入れると有効になります。
5	プリエンプトタイムアウト（秒）	ビデオセッションビューアにおいて、優先権のあるユーザーに接続を取られる際に表示されるダイアログ上で操作権を取られるまでのカウントダウン時間を指定します。 1～120（秒）の範囲で設定します。
共有		
6	”共有”、”自動”、”エクス	”有効” チェックボックスにチェックを入れるとビデオセッション

	クルーシブ”、”ステルス” チェックボックス	ビューアの共有操作が有効になります。 📖 参照 4.18 共有モード（207 ページ） ”自動” チェックボックスにチェックを入れるとビデオセッションビューアを共有モードで接続する際に、先に接続していたユーザーに対して通知することなく、接続が実行されます。 ”エクスクルーシブ” チェックボックスにチェックを入れるとビデオセッションビューア起動中にエクスクルーシブモードを有効にすることができ、他のユーザーの接続を拒否することができます。 📖 参照 4.17 エクスクルーシブモード（204 ページ） ”ステルス” チェックボックスにチェックを入れるとビデオセッションビューアで共有接続する際にステルスモードでの接続を選択することができるようになります。 ステルスモードとは、優先ユーザーに認識されることなく、ビデオ表示のみを共有する接続モードです。 📖 参照 4.19 ステルスモード（210 ページ）
7	入力制御のタイムアウト	共有モードで接続している場合、ユーザーA が制御を終了した後、ユーザーB に制御が移るまでの遅延時間を指定します。1〜50（1/10 秒）の範囲で指定します。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

3.25. KVM セッションの設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「セッション」-「KVM」をクリックすると「アプライアンス KVM セッションの設定」ページが表示されます。セッションビューアにおいて送受信されるデータの暗号化やモニター解像度、キーボード言語レイアウトに関する設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
暗号化レベル		
1	キーボード/マウス	キーボード、マウスデータの暗号化モードを以下から選択します。 "128 ビット SSL(ARCFOUR)"、"DES"、"3DES"、"AES"
2	ビデオ	ビデオデータの暗号化モードを以下から選択します。 "128 ビット SSL(ARCFOUR)"、"DES"、"3DES"、"AES"
ハードウェアの提示		
3	キーボード	ターゲットデバイスへ入力するキーボードの言語レイアウトを選択します。
4	デフォルトのモニター解像度	ビデオセッションビューアのデフォルトのモニター解像度を以下から選択します。 "標準-1024x768(4:3)"、"ワイドスクリーン-1440x900(16:10)"

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

3.26. バーチャルメディアセッションの設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「セッション」-「バーチャルメディア」をクリックすると「アプライアンスバーチャルメディアセッションの設定」ページが表示されます。バーチャルメディアセッションのアクセスモードや送受信データの暗号化に関する設定を行うことができます。

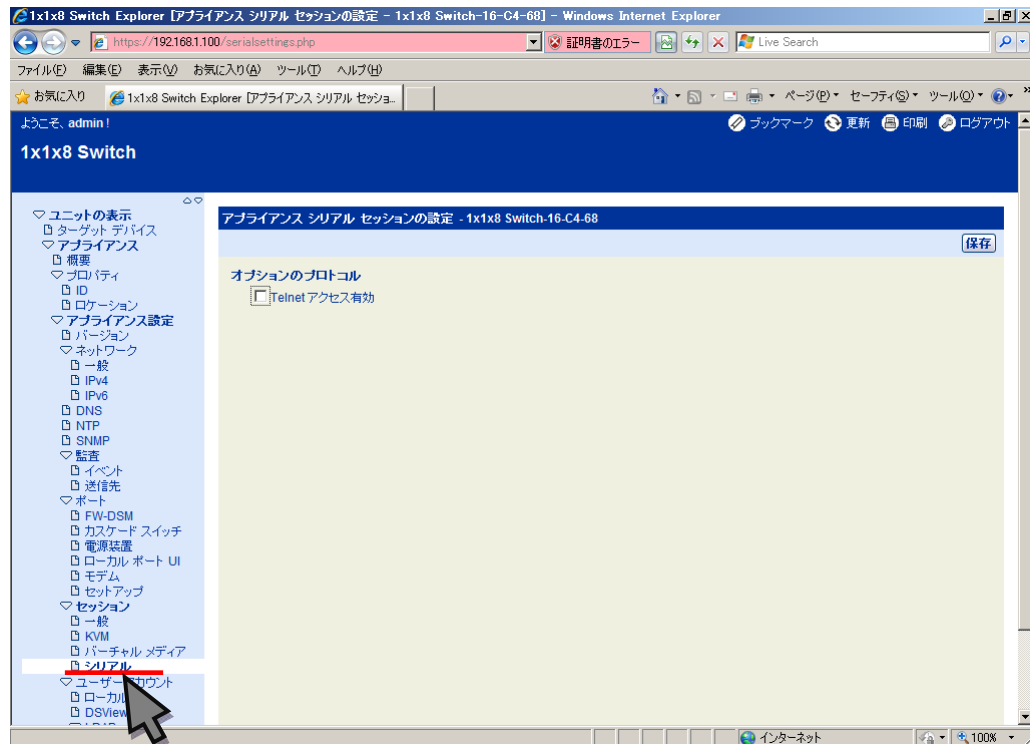
設定詳細は、下記のとおりです。

項	表示項目	内容
セッションの設定		
1	"バーチャルメディアが KVM セッションにロック" チェックボックス	本チェックボックスにチェックを入れるとビデオセッションビューアを終了する際に、バーチャルメディアセッションも同時に終了します。
2	"予約済みセッションを許可" チェックボックス	本チェックボックスにチェックを入れるとバーチャルメディアセッション実行時に他のユーザーからの接続を拒否することができます。
ドライブのマッピング		
3	バーチャルメディアアクセスモード	マッピングされたバーチャルメディアへのアクセスモードを選択します。 "読み取り専用" を選択すると読み取りのみのアクセスとなります。 "読み取り/書き込み" を選択すると読み取りおよび書き込み可能なモードでのアクセスとなります。
暗号化レベル		
4	バーチャルメディア	バーチャルメディアセッションで有効にする暗号化レベルを以下から選択します。 "なし"、"128 ビット SSL(ARCFOUR)"、"DES"、"3DES"、"AES"
サーバーユニットを介したバーチャルメディアアクセス		

5	VM を有効にする	設定するサーバーユニットを選択し、本ボタンをクリックするとバーチャルメディア機能が有効になります。
6	VM を無効にする	設定するサーバーユニットを選択し、本ボタンをクリックするとバーチャルメディア機能が無効になります。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

3.27. シリアルセッションの設定

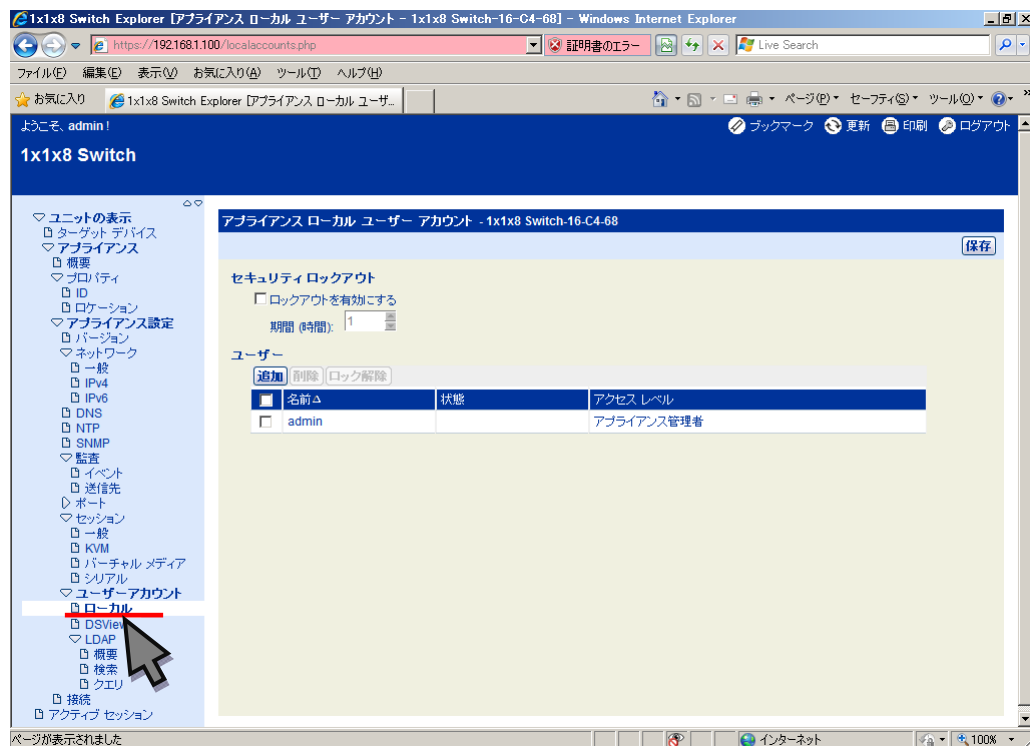
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「セッション」-「シリアル」をクリックすると「アプライアンス シリアルセッションの設定」ページが表示されます。ターゲットがシリアルデバイスの場合の Telnet アクセスに関する設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
オプションのプロトコル		
1	"Telnet アクセス有効"チェックボックス	本チェックボックスにチェックを入れるとシリアルデバイス用サーバーユニットが接続されたシリアルデバイスへの Telnet によるダイレクトアクセスが有効になります。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

Telnet アクセスから、ユーザー名、ターゲットデバイス名称、ユーザーパスワードの入力により、シリアルデバイスをダイレクトに制御することができます。
Telnet アクセスの方法については、下記をご参照ください。
📖 参照 4.20.6 Telnet によるシリアルアクセス（222 ページ）

3.28. ローカルユーザーの設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ユーザーアカウント」-「ローカル」をクリックすると「アプライアンスローカルユーザーアカウント」ページが表示されます。ローカルユーザーに関する設定を行うことができます。本ページでは、現在登録されているユーザーが一覧表示されます。
デフォルトでは、アプライアンス管理者権限の "admin" のみが登録されています。

設定詳細は、下記のとおりです。

項	表示項目	内容
セキュリティロックアウト		
1	"ロックアウトを有効にする" チェックボックス	本チェックボックスにチェックを入れるとロックアウト設定が有効になります。 ロックアウト設定が有効になると 6 回連続でログインエラーが発生した場合、そのユーザーは指定の期間ロックアウト状態となり、ログインすることができません。 管理者は、ロックを解除することができます。
2	期間（時間）	ロックアウトする期間を 1～99（時間）の範囲で指定します。
ユーザー		
3	追加	新規ユーザーを登録します。
4	削除	登録ユーザーを削除します。
5	ロック解除	ロックアウトされているユーザーのロックを解除します。

任意の設定を行い、右上の［保存］ボタンをクリックすると設定が反映されます。

3.29. ユーザーアクセスレベル

本装置のユーザーアクセスレベルには、"アプライアンス管理者"、"ユーザー管理者"、"ユーザー" の 3 種類があります。

- アプライアンス管理者

  本装置の全ての設定 および 全ての接続ターゲットデバイスの操作権限を持つユーザー。

- ユーザー管理者

  全ての接続ターゲットデバイスの操作権限を持つユーザー。

- ユーザー

  許可された接続ターゲットデバイスの操作権限を持つユーザー。

各アクセスレベルにおける操作権限詳細は下記のとおりです。

操作内容	アプライアンス管理者	ユーザー管理者	ユーザー
システム設定	○	×	×
ターゲットデバイスへのアクセス権の設定	○	○	×
ユーザーアカウントの追加、変更、削除	○ **＊1**	○ **＊2**	×
自分自身のパスワードの変更	○	○	○
ターゲットデバイスへのアクセス	○ **＊3**	○ **＊3**	× **＊4**

＊1 全てのアクセスレベルのユーザーに対して可能。
＊2 "ユーザー管理者" および "ユーザー" に対して可能。
＊3 全てのターゲットデバイスに対して可能。
＊4 アクセス権が割り当てられたターゲットデバイスに対してのみ可能。

3.29.1 ユーザーの追加

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ユーザーアカウント」-「ローカル」をクリックすると「アプライアンスローカルユーザーアカウント」ページが表示されます。
ユーザー項目のリストに現在登録されているユーザーが表示されます。

［追加］ボタンをクリックします。

下のようなページが表示されます。

アプライアンス ローカル ユーザー アカウントの追加 - 1x1x8 Switch-16-C4-68
保存 キャンセル
アプライアンス ローカル ユーザー情報
ユーザー名: User01
パスワード: ••••••
パスワードの確認: ••••••
アクセス レベル: ユーザー
利用可能なターゲット デバイス
割り当てられたターゲット デバイス
520742-00006F
追加 ▶
◀ 削除
* ユーザー管理者とアプライアンス管理者はすべてのターゲット デバイスにアクセス可能です。

設定詳細は、下記のとおりです。

項	表示項目	内容
1	ユーザー名	新規登録するユーザー名を指定します。使用できるのは、A-Z、a-z、0-9、ハイフン(-)のみで、3 文字以上に設定する必要があります。
2	パスワード、 パスワードの確認	ユーザーパスワードを指定します。使用できるのは、A-Z、a-z、0-9、ハイフン(-)のみで、最低 5 文字の長さで、かつ大文字(A-Z)、小文字(a-z)、数字(0-9)を1つずつ含んでいる必要があります。
3	アクセスレベル	ユーザーのアクセスレベルを指定します。 ・アプライアンス管理者 ・ユーザー管理者 ・ユーザー

4	利用可能なターゲットデバイス 割り当てられたターゲットデバイス	アクセスレベルが "ユーザー" の場合に、アクセスを許可するターゲットデバイスを選択します。 "利用可能なターゲットデバイス" には、現在オンライン状態のサーバーユニットの EID が表示されます。 任意のサーバーユニットを選択し、[追加]ボタンをクリックして "割り当てられたターゲットデバイス" 側に追加することでそのターゲットデバイスへのアクセスが可能となります。

任意の設定を入力し、右上の[保存]ボタンをクリックすると新規ユーザーが登録されます。
ユーザー登録が完了すると、以下のようにユーザーの一覧表示に追加されます。

アプライアンス管理者、およびユーザー管理者は、接続されている全てのターゲットデバイスへアクセスすることができます。

3.29.2 ユーザー設定の変更

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ユーザーアカウント」-「ローカル」をクリックすると「アプライアンスローカルユーザーアカウント」ページが表示されます。
ユーザー項目のリストに現在登録されているユーザーが表示されます。

設定変更を行うユーザー名称をクリックします。下の例では、User01 という名称のユーザーの設定を変更します。

下のようなページが表示されます。ここでパスワード、ユーザーアクセスレベル および ユーザーアクセスレベルが ”ユーザー” の場合は、そのアクセス可能なターゲットデバイスの設定を変更することができます。

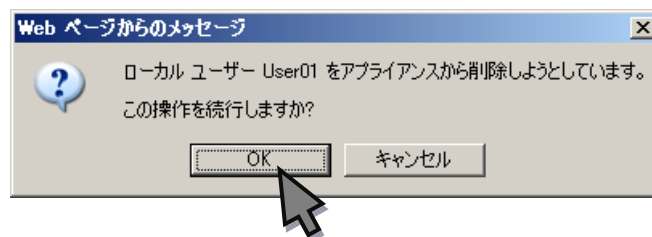
アプライアンス ローカル ユーザー アカウントの設定 - 1x1x8 Switch-16-C4-68 User01
保存 閉じる
アプライアンス ローカル ユーザー情報
ユーザー名: User01
パスワード:
パスワードの確認:
＊同じパスワードを使用する場合はパスワードを空欄のままにしてください。
アクセス レベル: ユーザー
利用可能なターゲット デバイス
割り当てられたターゲット デバイス
520742-00006F
追加 ►
◄ 削除
＊ユーザー管理者とアプライアンス管理者はすべてのターゲット デバイスにアクセス可能です。

任意の設定を入力し、右上の[保存]ボタンをクリックするとユーザー設定が変更されます。

3.29.3 ユーザーの削除

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ユーザーアカウント」-「ローカル」をクリックすると「アプライアンスローカルユーザーアカウント」ページが表示されます。
ユーザー項目のリストに現在登録されているユーザーが表示されます。

削除するユーザーのチェックボックスにチェックを入れ、[削除]ボタンをクリックします。

下のような確認メッセージが表示されます。削除する場合は、[OK]ボタンをクリックします。

ユーザーの削除が完了すると、ユーザー項目のリストから指定したユーザーの表示が削除されます。

3.29.4 セキュリティロックアウトの設定および解除

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ユーザーアカウント」-「ローカル」をクリックすると「アプライアンスローカルユーザーアカウント」ページが表示されます。

本ページにおいて、セキュリティロックアウトに関する設定を行うことができます。
セキュリティロックアウトとは、6 回連続でログインエラーが発生するとそのユーザーは指定の期間ロックアウト状態となり、下のようにログインページからログインすることができなくなる機能です。

ユーザー ログイン
*このページにはエラーが含まれています
間違ったログイン入力を何回も繰り返したため、このユーザーはロックアウトされています。
ユーザー名: Test01
パスワード:
言語: 日本語
ログイン

ロックアウト機能を有効にするには、"ロックアウトを有効にする" チェックボックスにチェックを入れ、右上の[保存]ボタンをクリックします。ロックアウト状態になったユーザーは、"期間" に設定された時間だけロックアウト状態が継続します。

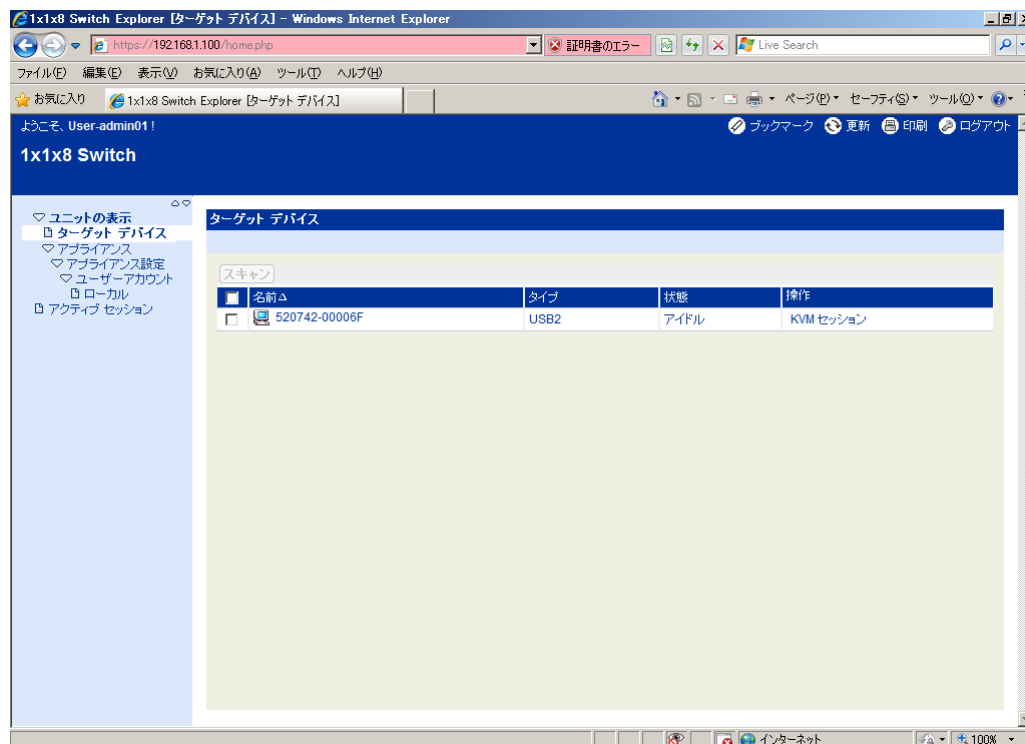
アプライアンス ローカル ユーザー アカウント - 1x1x8 Switch-16-C4-68
保存
セキュリティ ロックアウト
ロックアウトを有効にする
期間 (時間): 1

ロックアウト状態のユーザーを管理者ユーザーは、下のように確認することができます。
"Test01" ユーザーの状態項目に表示された 南京錠マークがロック状態であることを示します。

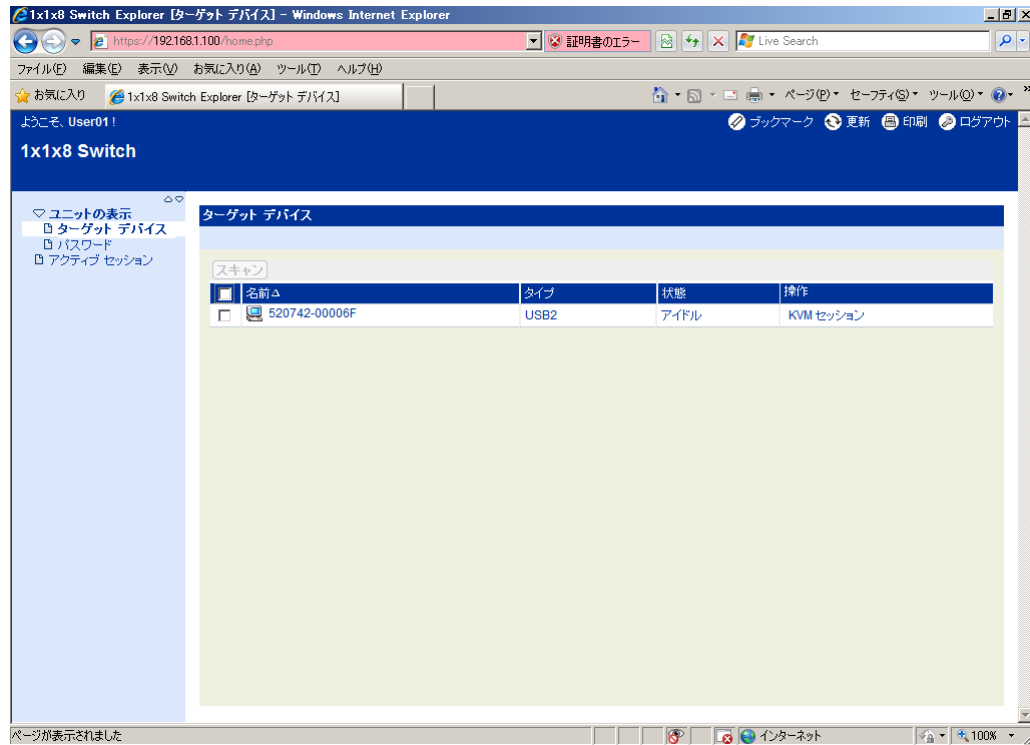
セキュリティロックを解除する場合は、そのユーザーのチェックボックスにチェックを入れ、[ロック解除]ボタンをクリックします。

下のように、南京錠マークが非表示となり、セキュリティロックアウトは解除されます。

3.29.5 ユーザー管理者権限での OBWI 操作

ユーザー管理者で OBWI にログインすると下のように画面左のメニュー選択領域が構成された表示が行われます。ユーザー管理者権限で操作可能な項目のみ表示された構成となります。

各項目の設定内容は、アプライアンス管理者での説明内容と同じです。

3.29.6 ユーザー権限での OBWI 操作

ユーザーで OBWI にログインすると下のように画面左のメニュー選択領域が構成された表示が行われます。ユーザー権限で操作可能な項目のみ表示された構成となります。

各項目の設定内容は、アプライアンス管理者での説明内容と同じです。

3.30. DSView 認証サーバーの設定

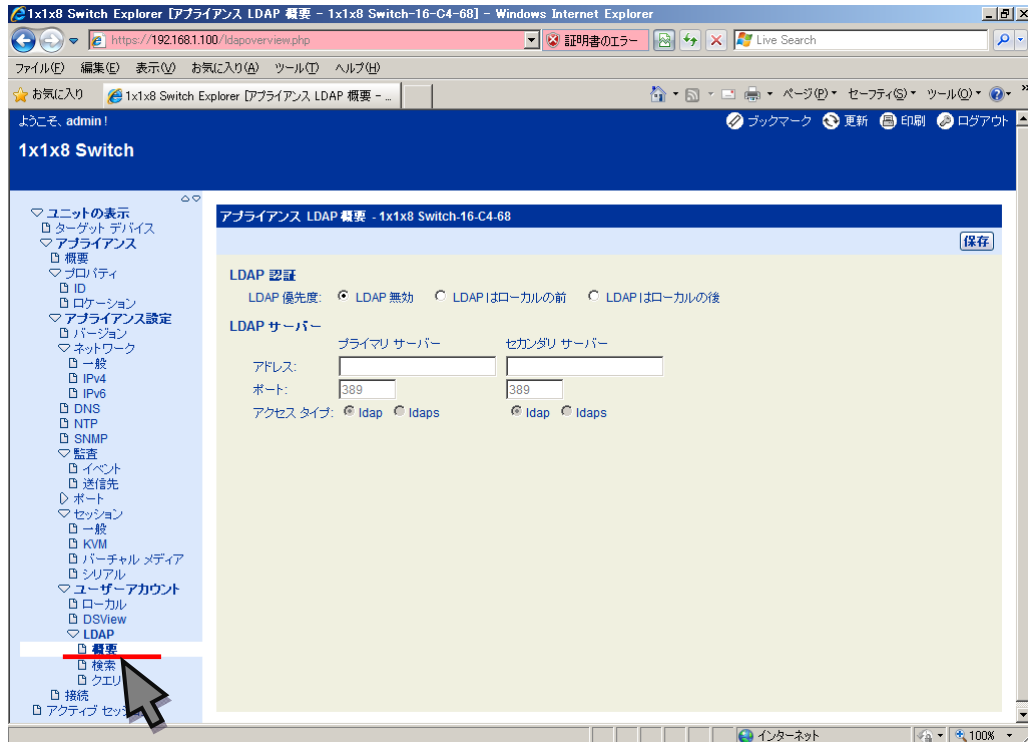
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ユーザーアカウント」-「DSView」をクリックすると「アプライアンス DSView 認証サーバーへの登録」ページが表示されます。DSView サーバーでの認証設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
1	サーバー	認証を行う DSView サーバーの IP アドレスを指定します。
2	再試行間隔（分）	認証に失敗した場合の再試行までの間隔（分）を指定します。

任意の設定を行い、右上の［保存］ボタンをクリックすると DSView サーバーでの認証が有効になります。［関連付けの解除］ボタンをクリックすると DSView サーバーでの認証が無効になります。

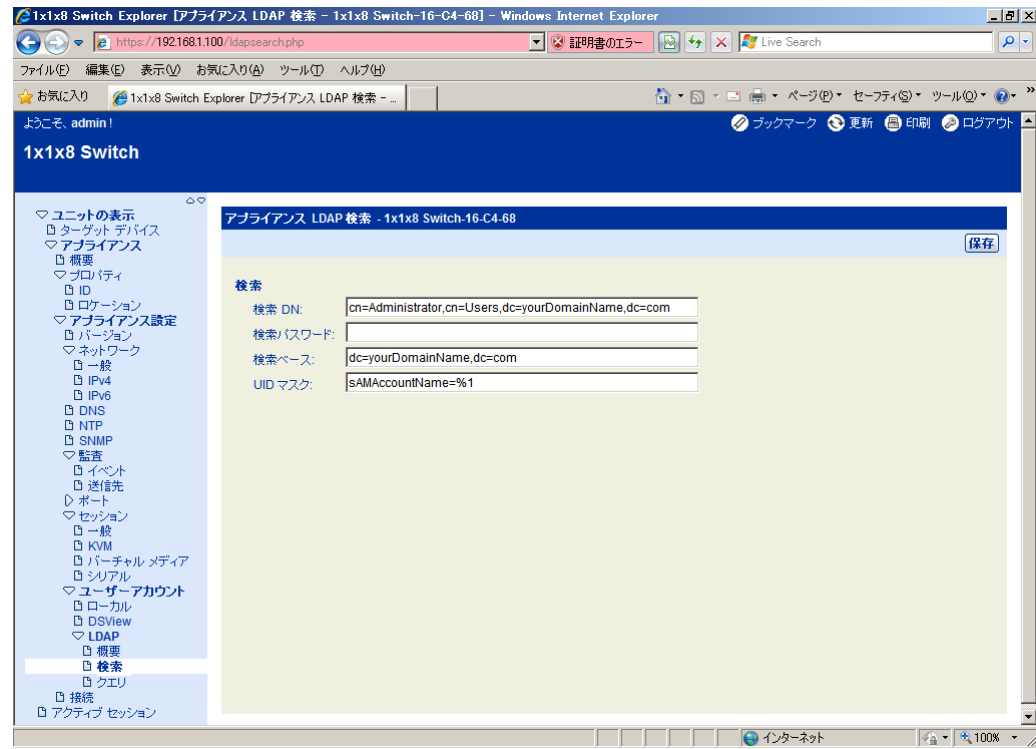
3.31. LDAP サーバーの一般設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ユーザーアカウント」-「LDAP」-「概要」をクリックすると「アプライアンス LDAP 概要」ページが表示されます。LDAP の有効/無効、LDAP サーバー設定を行うことができます。

設定詳細は、下記のとおりです。

項	表示項目	内容
LDAP 認証		
1	LDAP 優先度	認証の優先度を以下から選択します。 "LDAP 無効"： ローカル認証のみを実行します。 "LDAP はローカルの前"： まず LDAP 認証を実行し、LDAP 認証に失敗した場合、その後ローカル認証を実行します。 "LDAP はローカルの後"： まずローカル認証を実行し、ローカル認証に失敗した場合、その後 LDAP 認証を実行します。
LDAP サーバー		
2	アドレス	LDAP サーバーの IP アドレスを指定します。 プライマリサーバー、セカンダリサーバーの 2 台まで設定することができます。
3	ポート	LDAP の TCP ポート番号を指定します。
4	アクセスタイプ	LDAP 認証のアクセスタイプを "ldap" あるいは "ldaps" のいずれかを選択します。"

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。
設定例として、以下をご参照ください。
📖 参照 3.36 Active Directory サーバーによる認証（150 ページ）

3.32. LDAP サーバーの検索設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ユーザーアカウント」-「LDAP」-「検索」をクリックすると「アプライアンス LDAP 検索」ページが表示されます。LDAP 認証の検索に関する設定を行うことができます。

設定詳細は、下記のとおりです。

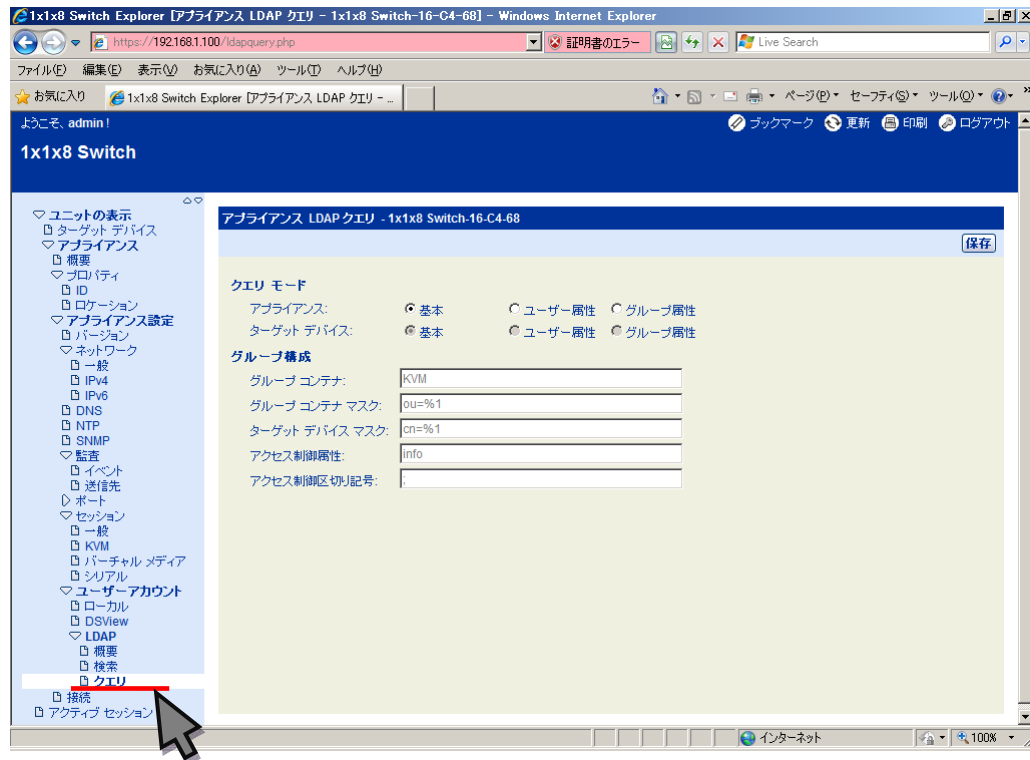
項	表示項目	内容
1	検索 DN	ディレクトリと、その操作権限を持つアカウント(Administrator)の所在を記述します (User に属する Administrator)。 本装置が LDAP サーバーに対して Administrator でログインした後、ディレクトリを検索するのに必要な情報です。
2	検索パスワード	ディレクトリの操作権限を持つアカウント(Administrator) のパスワードを記述します。
3	検索ベース	ディレクトリのパスを記述します。
4	UID マスク	LDAP サーバーから読み取るユーザー名のコンテナを記載します。sAMAccountName となっています。"=%1" は内部動作に必要ですので、この記述形式を守ってください。

任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

設定例として、以下をご参照ください。

📖 参照 3.36 Active Directory サーバーによる認証（150 ページ）

3.33. LDAP サーバーのクエリ設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ユーザーアカウント」-「LDAP」-「クエリ」をクリックすると「アプライアンス LDAP クエリ」ページが表示されます。LDAP 認証のクエリに関する設定を行うことができます。

設定詳細は、下記のとおりです。

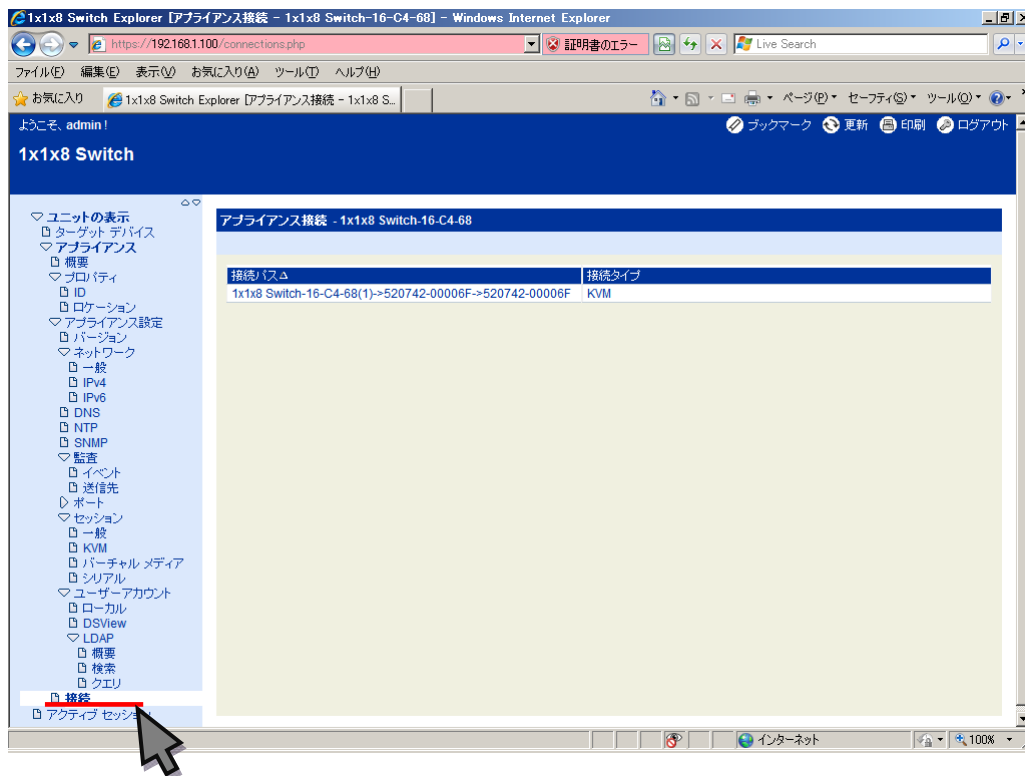
項	表示項目	内容
クエリモード		
1	アプライアンス	本装置のクエリモードを選択します。
2	ターゲットデバイス	ターゲットデバイスのクエリモードを選択します。
グループ構成		
3	グループコンテナ	グループコンテナを指定します。
4	グループコンテナマスク	グループコンテナマスクを指定します。
5	ターゲットデバイスマスク	検索する属性から値を取得するための記述です。
6	アクセス制御属性	ユーザーおよびグループのアクセス権限を示す属性名を指定します。
7	アクセス制御区切り記号	アクセス制御の区切り記号を指定します。

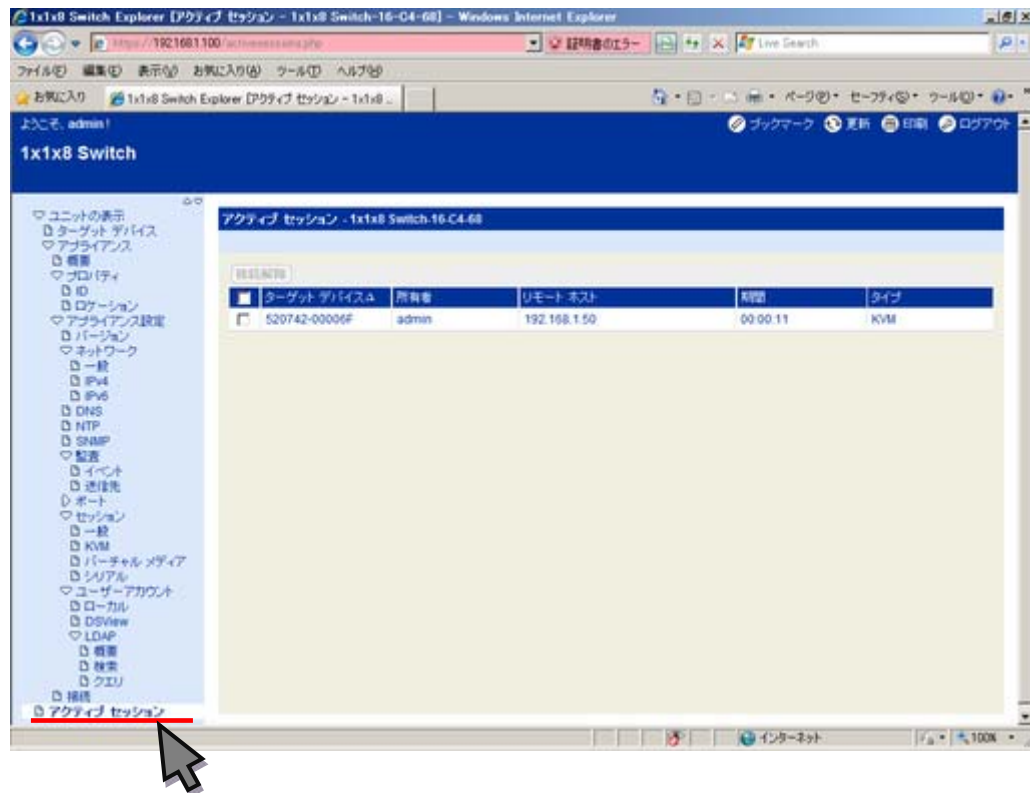
任意の設定を行い、右上の[保存]ボタンをクリックすると設定が反映されます。

設定例として、以下をご参照ください。

📖 参照 3.36 Active Directory サーバーによる認証（150 ページ）

3.34. 接続パスの確認

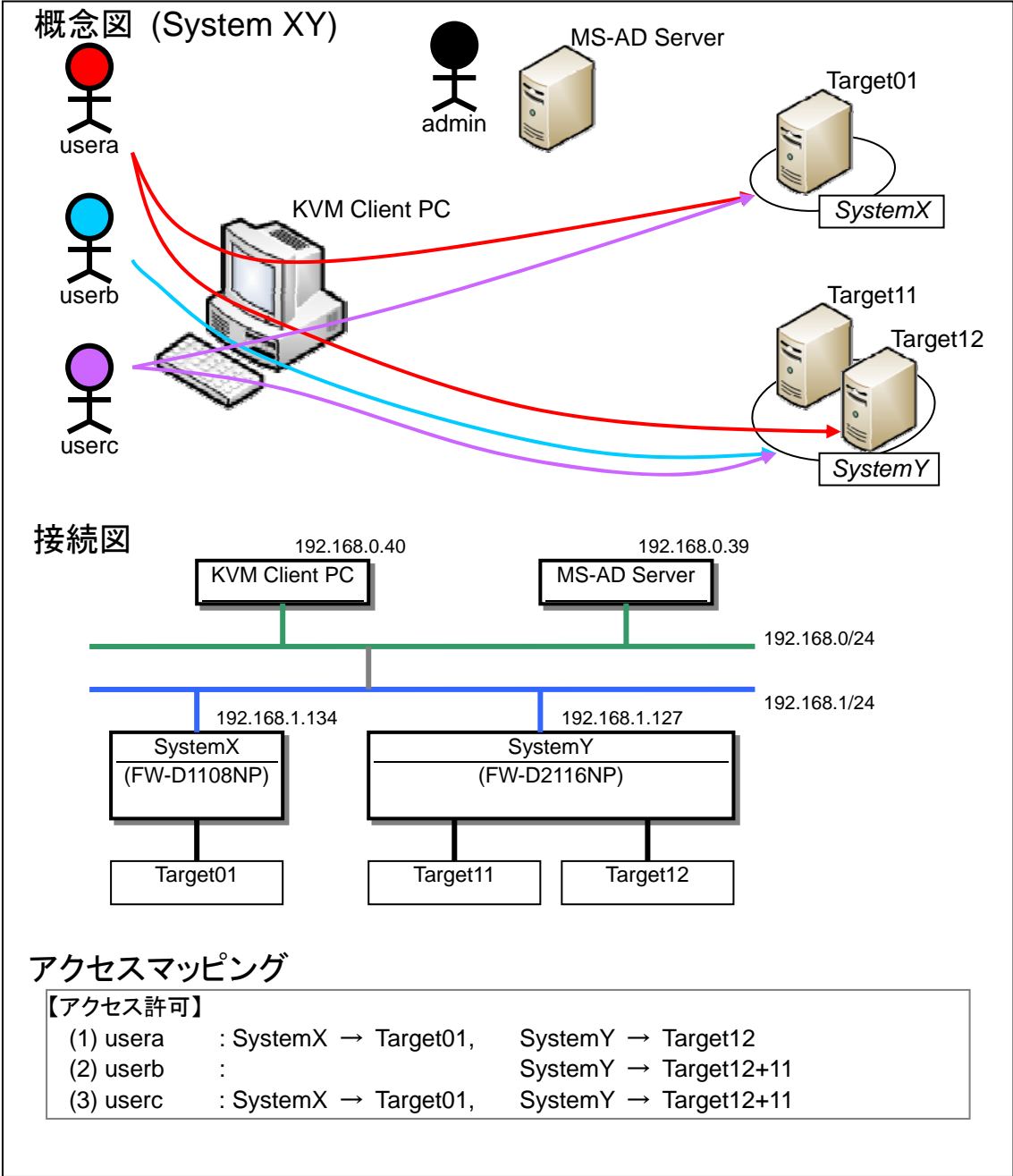
画面左のメニュー選択領域において、「ユニットの表示」-「接続」をクリックすると「アプライアンス接続」ページが表示されます。接続サーバーユニットの接続パス、接続タイプを確認することができます。

3.35. アクティブセッションの確認

画面左のメニュー選択領域において、「アクティブセッション」をクリックすると「アプライアンス接続」ページが表示されます。現在ターゲットデバイスにアクセスしているリモートユーザーの情報などを確認することができます。

また、現在ターゲットデバイスにアクセスしているセッションを解除することができます。解除するセッション情報のチェックボックスにチェックを入れて、[接続解除]ボタンをクリックします。

指定されたセッションが切断され、アクティブセッションのリストからも削除されます。

3.36. Active Directory サーバーによる認証

LDAP 認証機能を使用する一例として、Active Directory サーバーを用い 複数の本装置に有効なアカウントとアクセス権の設定および運用方法について説明します。
なお、本説明にて使用する Activi Directory サーバーの構築において、Windows サーバーと Active Directory サーバー、DNS サーバーのインストール方法については、割愛させていただきます。

3.36.1 本書でのシステム構成

図の解説

MS-AD Server : Active Directory および DNS サーバーです。
本書では、Windows Server 2003 R2 を用いています。
このサーバーにアクセスできるのは管理者のみです。

KVM Client PC : 管理者を含む各 user が共通して利用する操作端末です。
この PC のアカウント管理方法は問いません。

SystemX : 1 ユーザーx8 サーバーの IP-KVM FW-D1108NP です。
System X という管理名が付けられています。
SystemY : 2 ユーザーx16 サーバーの IP-KVM FW-D2116NP です。
System Y という管理名が付けられています。

Target01 : Target 01 という管理名が付けられたサーバーです。
＊実際は、何れかのサーバーユニットに対して名前を設定。
Target11 : Target 11 という管理名が付けられたサーバーです。
＊実際は、何れかのサーバーユニットに対して名前を設定。
Target12 : Target 12 という管理名が付けられたサーバーです。
＊実際は、何れかのサーバーユニットに対して名前を設定。

---

usera : System X と Target 12 にアクセスできるユーザー。
userb : System Y にだけアクセスできるユーザー。
userc : System X と System Y にアクセスできるユーザー。

---

admin : システム全体の管理者で、どこにでもアクセスすることができます。

3.36.2 Active Directory システム設計

Active Directory を使って本装置のユーザーとアクセス権の管理を実現する場合、次の手順に沿って、定義していきます。

- 全体システム名の決定
  ↓
- 概念図の設計
  ↓
- 名称／アクセスマップ／接続図の管理
  ↓
- Active Directory サーバーの設定

まず全体のシステム名を最初に決めます。
この全体のシステム名を Active Directory サーバーで新規作成する OU の名前に用います。システム構成図にて、「System XY」と名付けました。

次にユーザーとサーバー、ユーザー毎のアクセス許可を考えながら「概念図」としてまとめます。概念図を作成後、各システムへ適用する本装置のモデルを決めるため、最大同時アクセス数を数えます。その結果、今回は 2 本繋がった SystemX には FW-D1108NP を、3 本繋がった SystemY には FW-D2116NP を割り当てることにしました。

各ハードウェアは決定したため、ネットワーク経路を含めて接続図として整理します。さらに、各ユーザーのアクセス経路をテーブル化します。

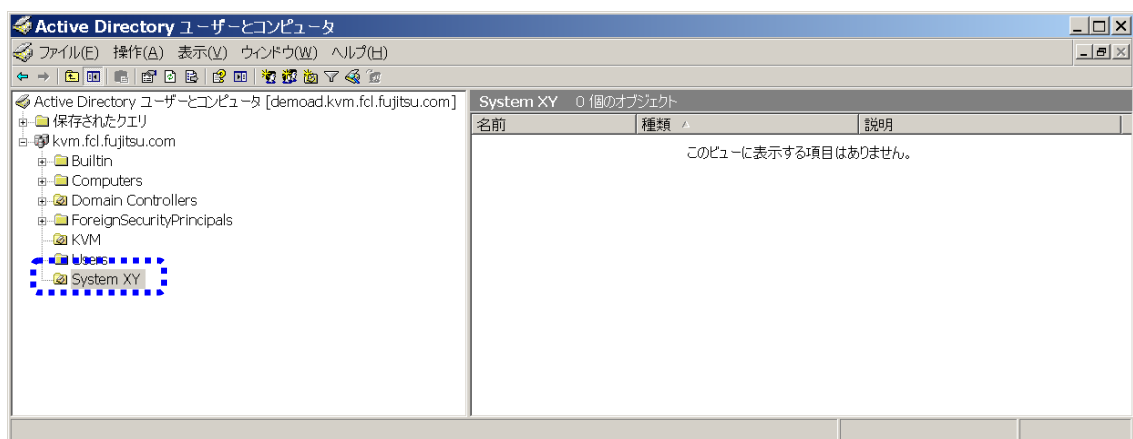
Active Directory サーバーを使った管理に必要な情報は、3.30.1 項の「アクセスマッピング」と Active Directory サーバーの IP アドレスの 2 点となります。

次項より、3.30.1 項のシステム構成図に従って、Active Directory サーバーの実際の設定手順を説明していきます。

3.36.3 Active Directory サーバーの設定

3.36.3.1 基本作業（OU の作成）

Active Directory サーバー（以下、AD サーバーと略します。）は既に構築済みとします。
ここでは kvm.fcl.fujitsu.com と言う DNS 名を持った既存の AD サーバーを使って説明していきます。
まず AD サーバーに対しては、全体システム名を使って OU を作成します。
コントロールパネルから「Active Directory ユーザーとコンピュータ」を開き、「kvm.fcl.fujitsu.com」と言う DNS 名（今回の例）の上で右クリックし、新規作成 ＞ 組織単位(OU) を選択します。

開いたウィンドウで、3.30.2 項で定めた全体システム名「System XY」を入力して完了します。

3.36.3.2 ユーザーの登録

作成するユーザーは ”usera”, ”userb”, ”userc” です。
これらユーザーは管理者ではなく一般ユーザーとなりますので、下に示す 本装置で識別可能な属性から KVM User を選ぶことにします。

アプライアンス管理者	:	KVM Appliance Admin
ユーザー管理者	:	KVM User Admin
ユーザー	:	KVM User

管理者には KVM Appliance Admin の属性を付けます。

「System XY」OU の中で ユーザー を新規作成します。

usera 作成開始　　　　　usera パスワード登録

姓名の欄には適当で構いませんが、「ユーザーログオン名」の欄に、正しいユーザー名「usera」を入力して下さい。入力が完了したら「次へ」ボタンをクリックして、パスワードを設定します。今回は ”usera” と言うパスワードを設定しました。

次に、”usera” の上で右クリックして、プロパティを開き、「電話」タブを表示し、今回 ”usera” の権限として選択した「KVM User」を「メモ(N)」欄に記載して完了します。

usera プロパティ表示　　　　　usera 電話タブ表示

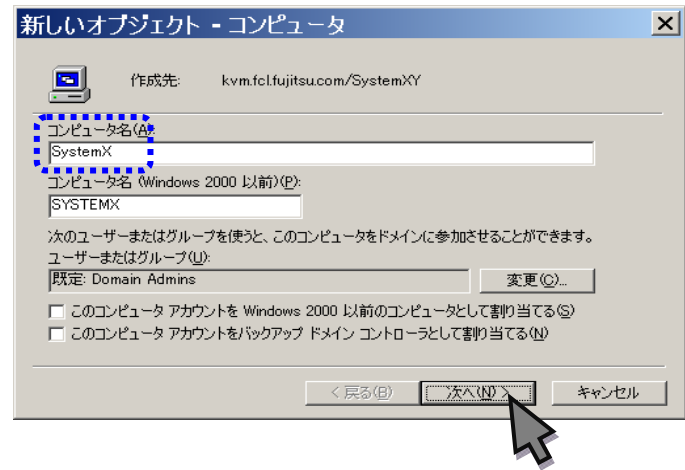
解 説

本装置が LDAP サーバーに対してユーザー名を問い合わせする際、「sAMAccountName フィールド」を問い合わせてきます。Active Directory サーバーでの「sAMAccountName フィールド」とは、ユーザーのプロパティのアカウントタブにある「ユーザーログオン名（Windows2000 以前）」欄に該当します。
同様に、本装置が LDAP サーバーに対してユーザー権限を問い合わせする際、「info フィールド」を問い合わせてきます。Active Directory サーバーでの「info フィールド」は、ユーザーのプロパティの電話タブにある「メモ」欄に該当します。

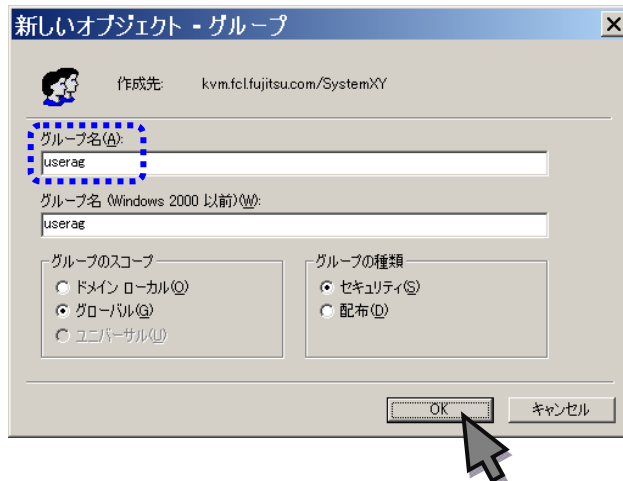
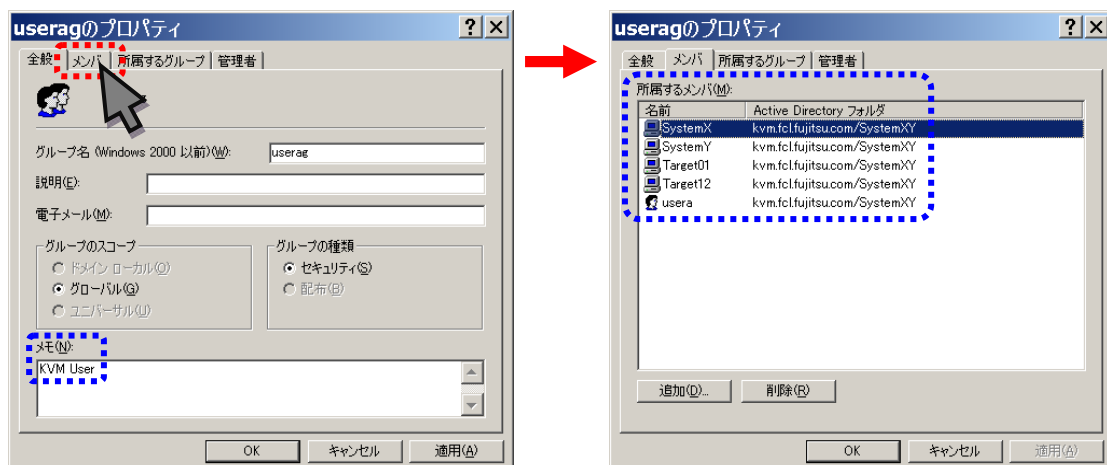
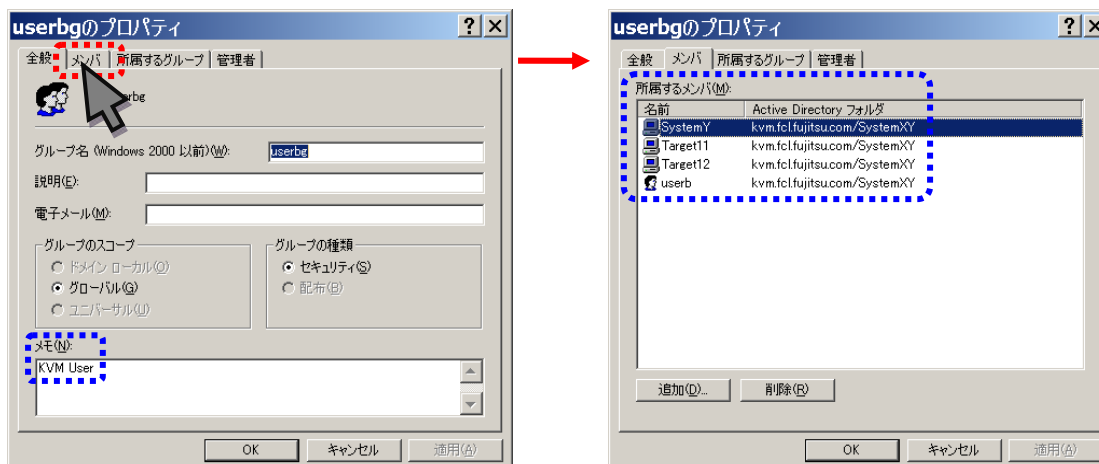
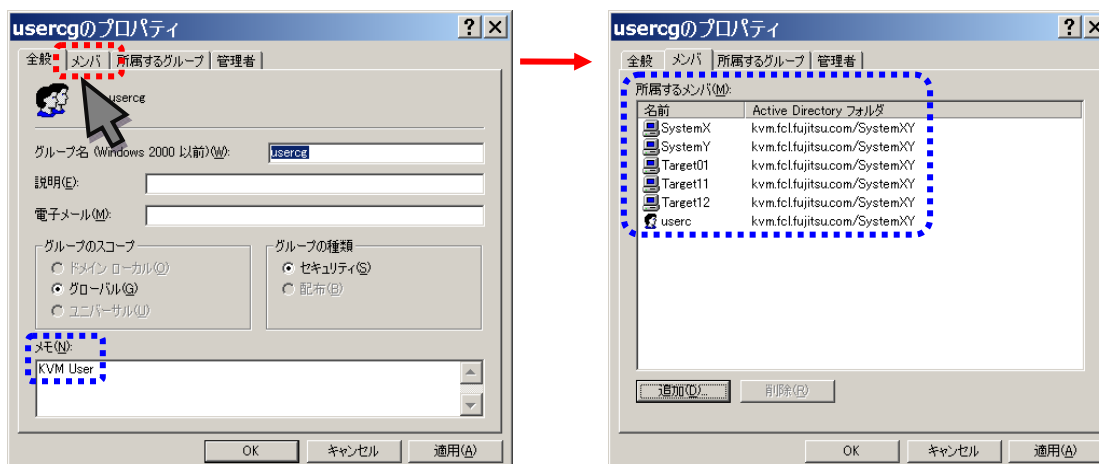
3.36.3.3 コンピュータの登録

次に、「System XY」で管理対象とする下記一覧のハードウェアを登録します。

ハードウェア	管理名
IP-KVM FW-D1108NP 本体	SystemX
IP-KVM FW-D2116NP 本体	SystemY
サーバー Target 01	Target01
サーバー Target 11	Target11
サーバー Target 12	Target12

Active Directory において、各ハードウェアは全て「コンピュータ」で管理します。
まず「SystemX」を登録するため、「System XY」の上で右クリックし、「新規作成」 ＞ 「コンピュータ」 を選択します。
コンピュータ名に「SystemX」と入力したら、「次へ」 ＞ 「次へ」 ＞ 「完了」 の順でボタンをクリックします。

他のハードウェアも同様に作成してください。
各コンピュータは作成するだけで良く、プロパティ等は調整する必要はありません。

3.36.3.4 グループの登録

続いて、ユーザーとコンピュータをまとめるユーザーグループを作成します。Active Directory サーバーでユーザーとハードウェアを登録しただけでは、3.30.1 項で定めたアクセスマッピングは設定できていませんので、各ユーザーは SystemX と SystemY にログインすることしか出来ません。
まず ”usera” のアクセスマップを作成するため、ユーザーやコンピュータの新規作成方法と同じように、「新規作成」 > 「グループ」 を選択してください。
開いたウィンドウのグループ名の欄に「userag」と入力して完了して下さい。

次に、作成した「userag」のプロパティを開き、メモ欄に「KVM User」と記載してください。
これは ”userag” も ”usera” と同じく権限の設定が必要になるためです。
次に「メンバ」タブを選択し、「追加」ボタンをクリックして、下に示すように、3.30.1 項で定義してある ”usera” に許可しているコンピュータと ”usera” 自身を登録してください。

”userbg” を同様に作成します。

”usercg” を同様に作成します。

以上で、AD サーバーの設定は完了です。

3.36.3.5 admin ユーザーについて

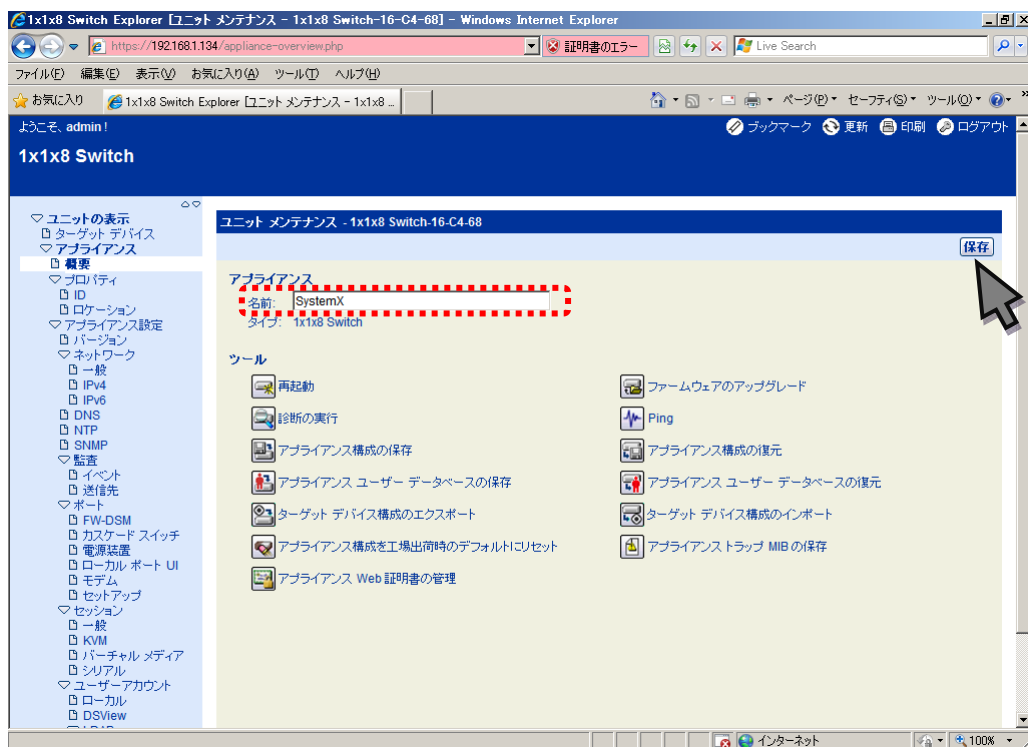
admin は本装置へのビルトインアカウントのため、AD サーバーで管理する必要はありませんが、KVM Appliance Admin を権限とする新しいユーザーを作成しても構いません。

3.36.4 本装置の設定

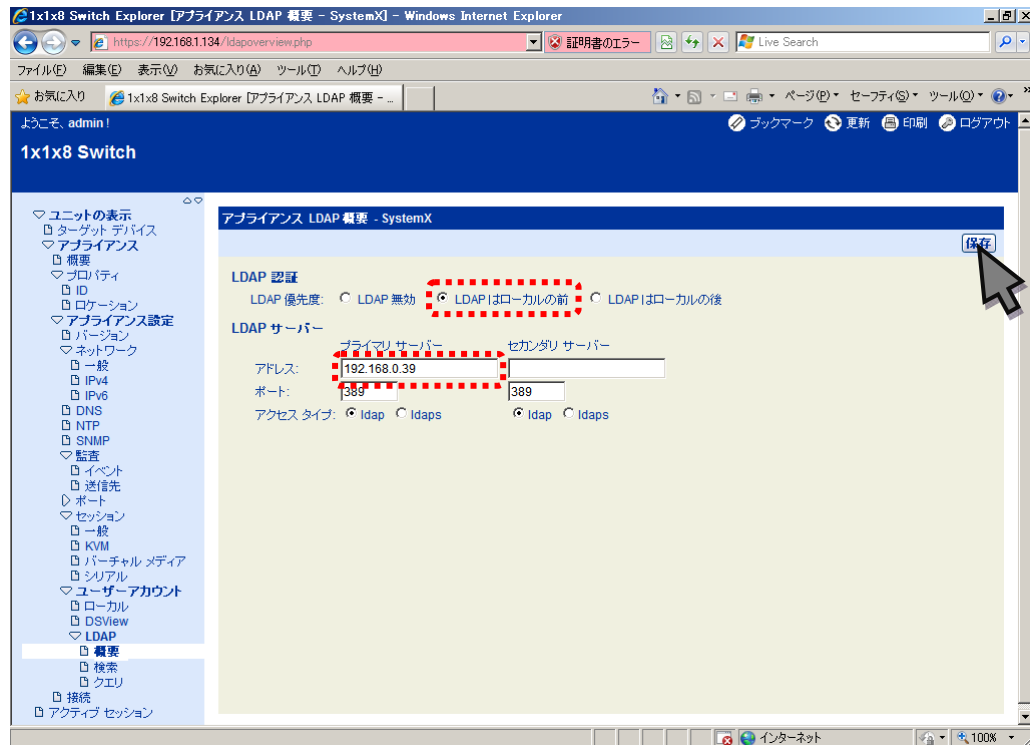
3.36.4.1 ユーザーの整理

Active Directory を使って認証を行う場合、本装置のユーザー設定では、デフォルトの admin 以外は不要です。

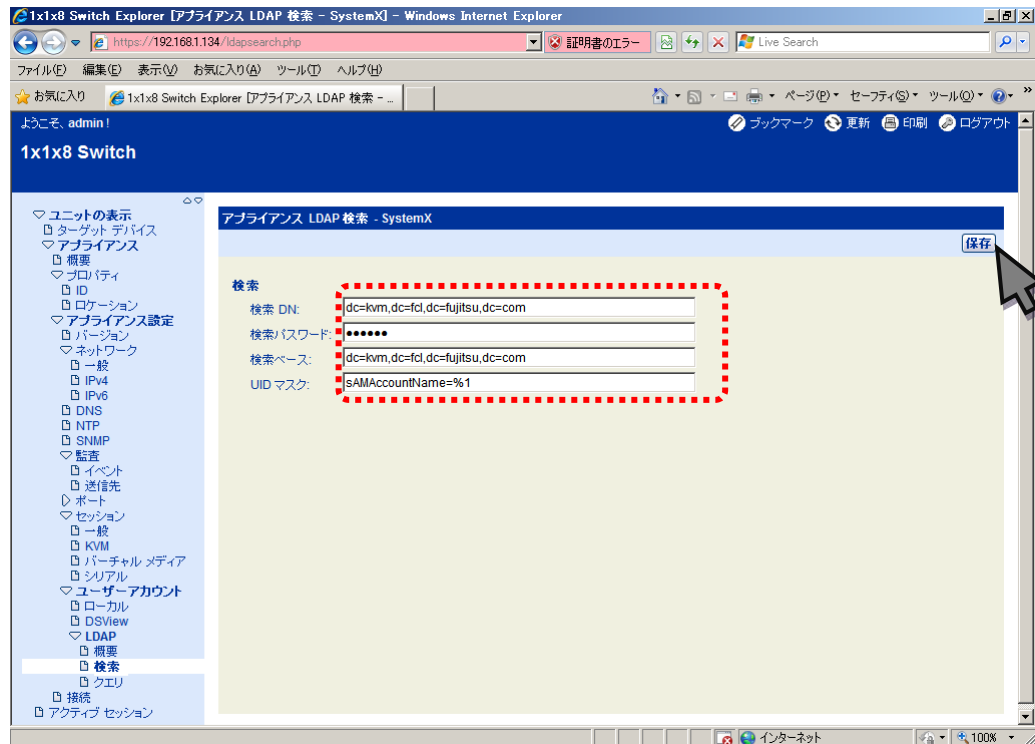
3.36.4.2 装置名の設定

3.30.2 項で設計した管理名「SystemX」となる FW-D1108NP を設定します。
ブラウザで、https://192.168.1.134/（IP アドレスは環境毎に異なります）開きます。
ビルトインアカウントの ”admin” でログイン後、画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「概要」をクリックすると「ユニットメンテナンス」ページが表示されます。「名前」項目に、管理名「SystemX」を入力します。

入力後に、画面右上にある「保存」ボタンをクリックします。

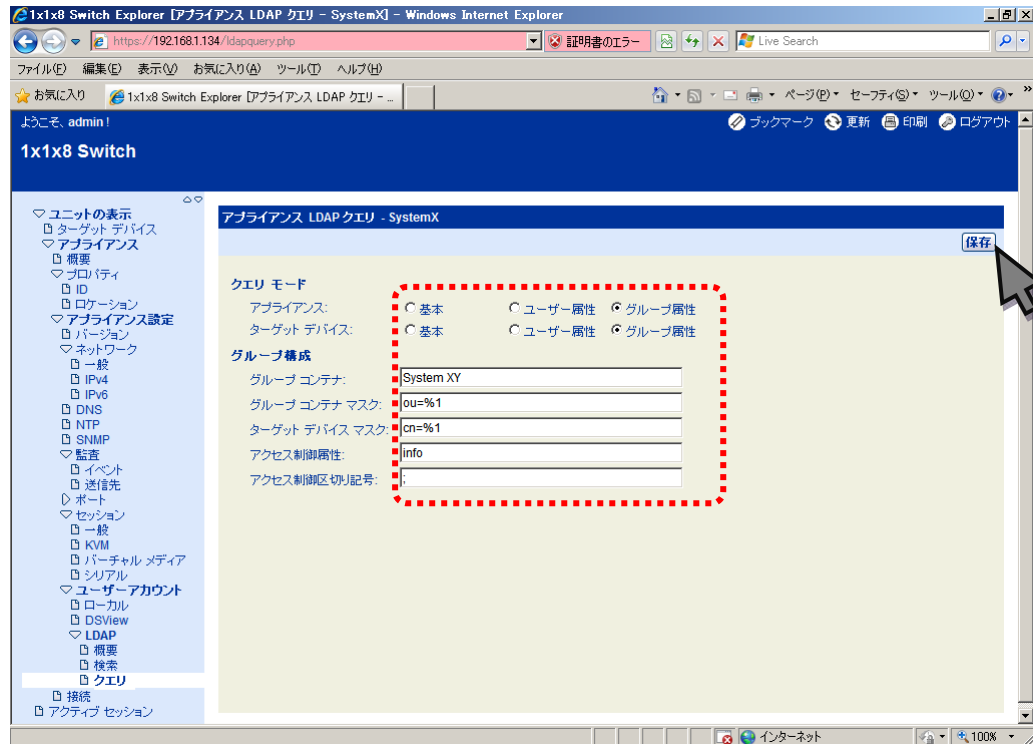
3.36.4.3 認証の設定

3.30.2 項で設定した Active Directory サーバーへのアクセス設定を行います。
画面左のメニュー選択領域において、｢ユニットの表示｣-｢アプライアンス｣-｢ユーザーアカウント｣-｢LDAP｣-｢概要｣をクリックすると｢アプライアンス LDAP 概要｣ページが表示されます。下記の通りに設定します。

LDAP サーバーを登録する時は｢LDAP 優先度｣項目において、”LDAP は、ローカルの前”を選択します。アドレス項目に、Active Directory サーバーの IP アドレスを入力し、右上の［保存］ボタンをクリックします。

本装置のデフォルトユーザーである ”admin” のアカウントは、本体で管理します。

続いて、検索項目について登録します。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「ユーザーアカウント」-「LDAP」-「検索」をクリックすると「アプライアンス LDAP 検索」ページが表示されます。

検索 DN	ディレクトリと、その操作権限を持つアカウント(Administrator)の所在を記述します。(User に属する Administrator)。 今回のディレクトリは「kvm.fcl.fujitsu.com」ですから、LDAP 風に記述すると「dc=kvm,dc=fcl,dc=fujitsu,dc=com」となります。 本装置が Active Directory サーバーに対して Administrator でログインした後、ディレクトリを検索するのに必要な情報です。
検索パスワード	ディレクトリの操作権限を持つアカウント(Administrator)のパスワードを記述します。
検索ベース	ディレクトリのパスを記述します。 今回のディレクトリは「kvm.fcl.fujitsu.com」ですから、LDAP 風に記述すると「dc=kvm,dc=fcl,dc=fujitsu,dc=com」となります。
UID マスク	Active Directory サーバーから読み取るユーザー名のコンテナを記載します。ユーザーの作成方法で説明したように、sAMAccountName となっています。 「=%1」は内部動作に必要ですから、この記述形式を守ってください。

記入後、右上の[保存]ボタンをクリックします。

続いて、”クエリ” 項目について登録します。
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「ユーザーアカウント」-「LDAP」-「検索」をクリックすると「アプライアンス LDAP 検索」ページが表示されます。

クエリモード　　今回は「グループ属性」を選択します。複数のアプライアンスと複数のサーバーを 3 つのユーザーで振り分けているので両方がグループ属性を必要とします。

グループコンテナ　**最初に作った ”System XY” を記述します。**

グループコンテナマスク
今回は OU をコンテナとしているため、 ”ou=%1” になります。

ターゲットマスク　　検索する属性（例えば info や sAMAccountName など）から値を取得するための記述です。変更は不要です。

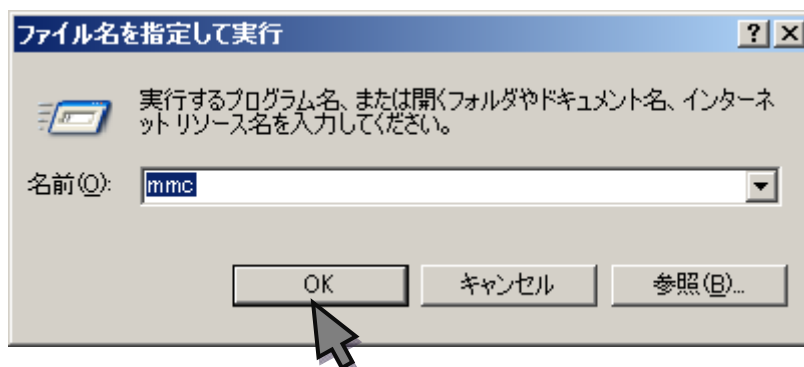
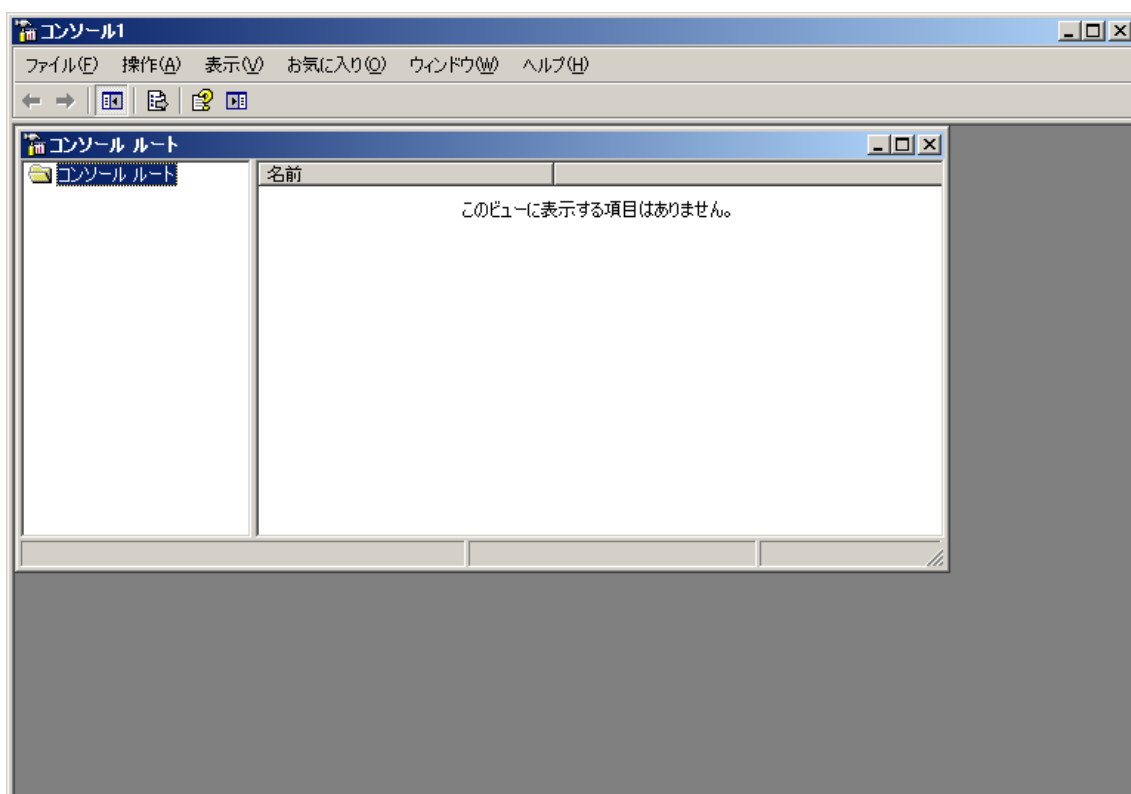
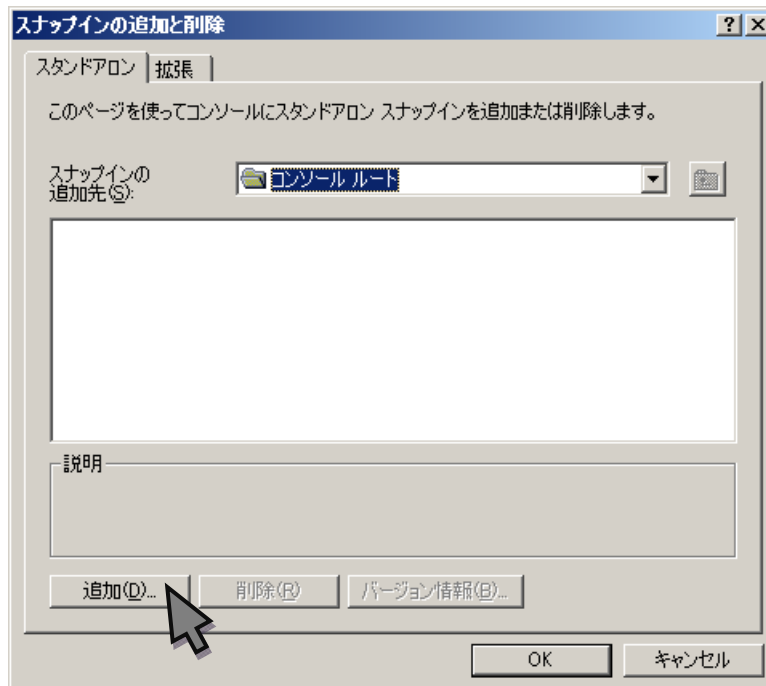
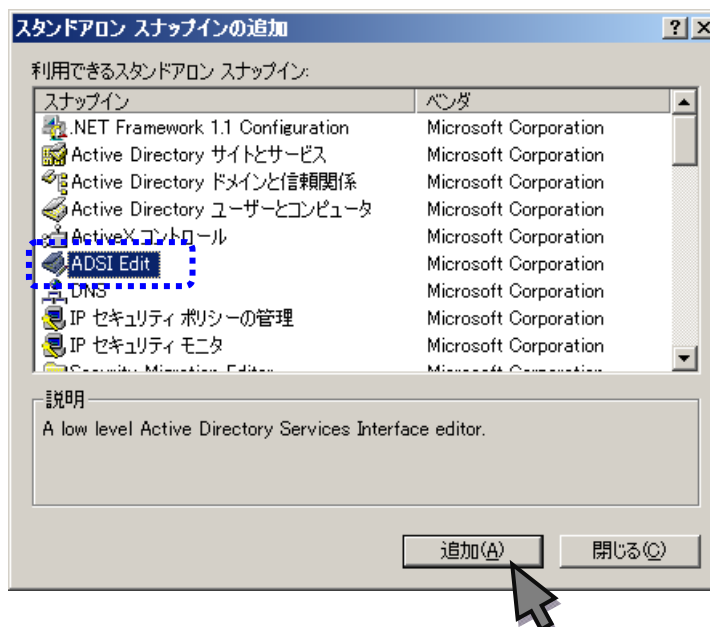
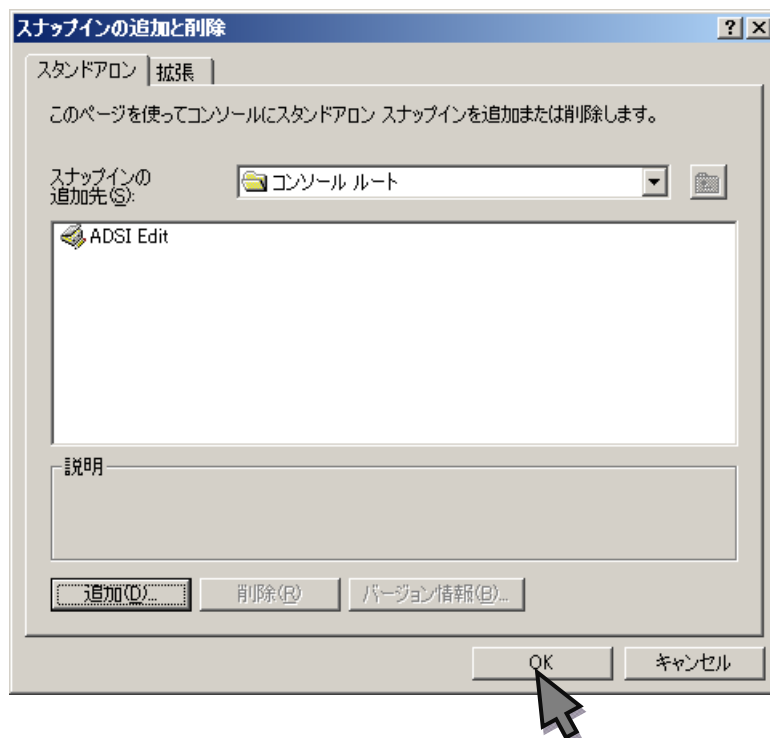
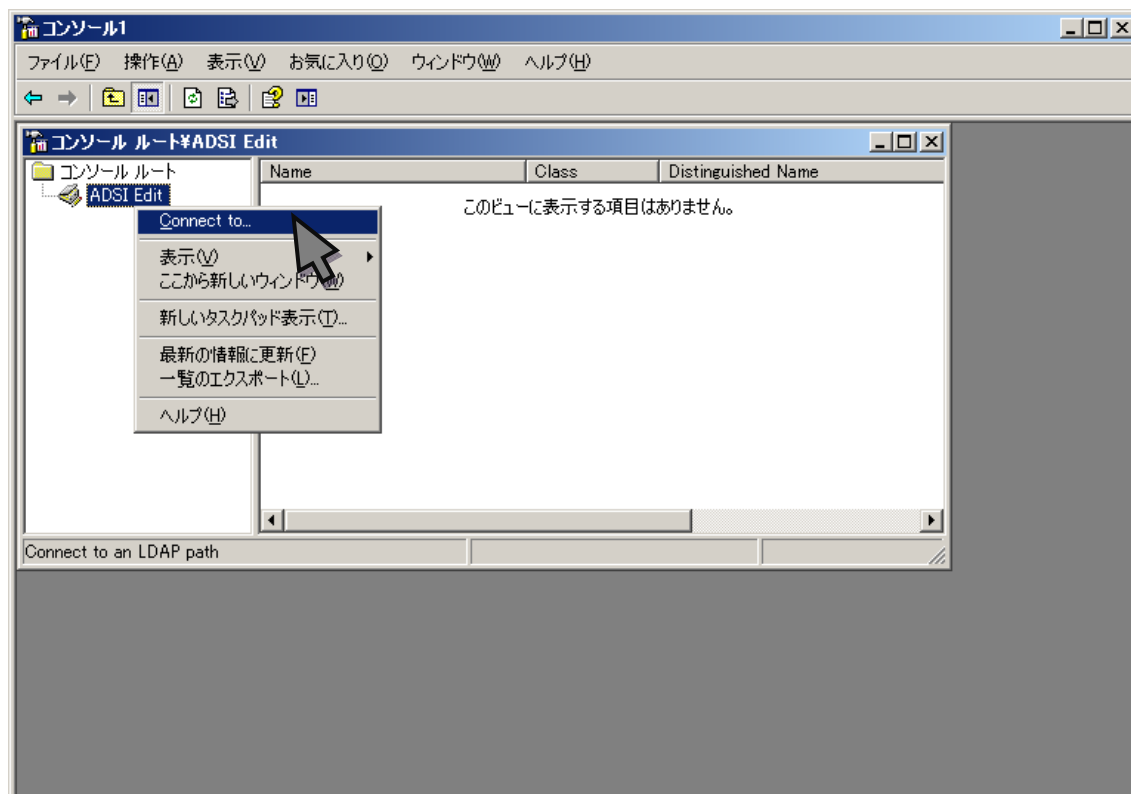
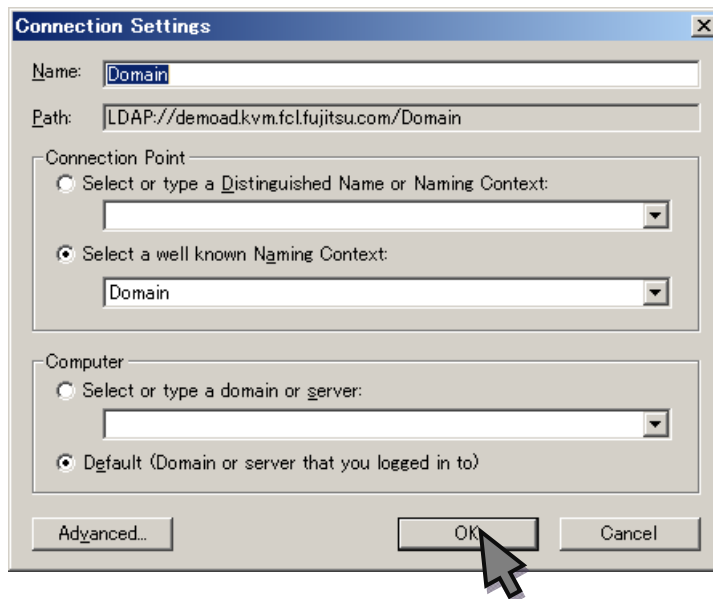
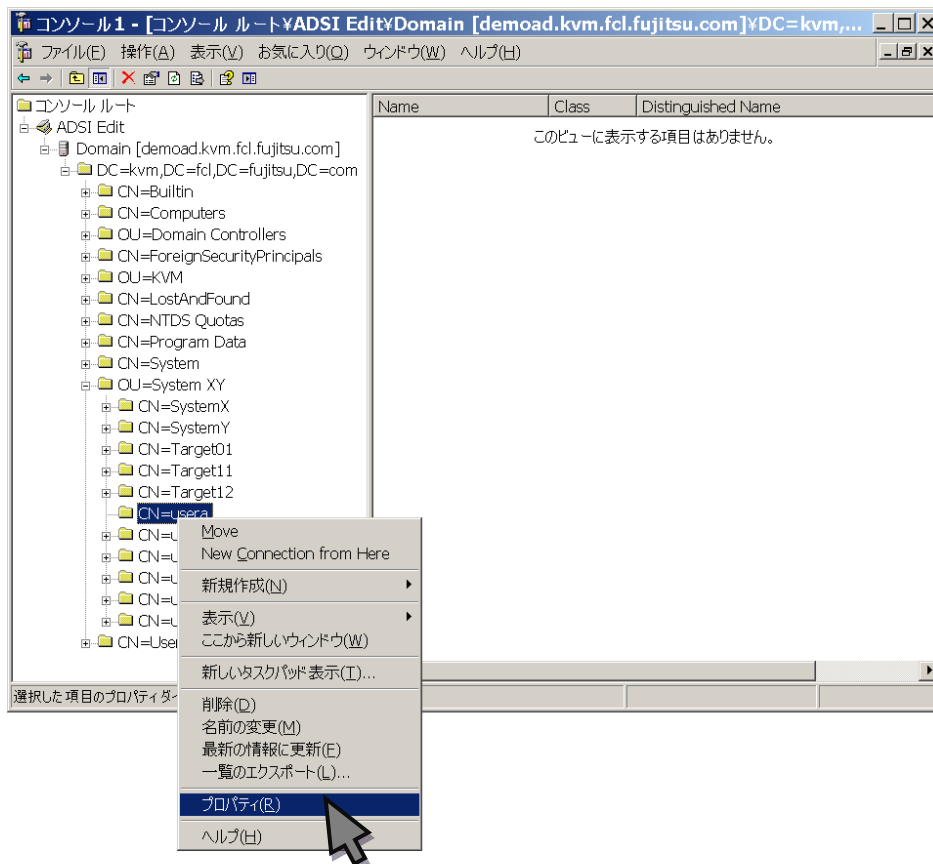
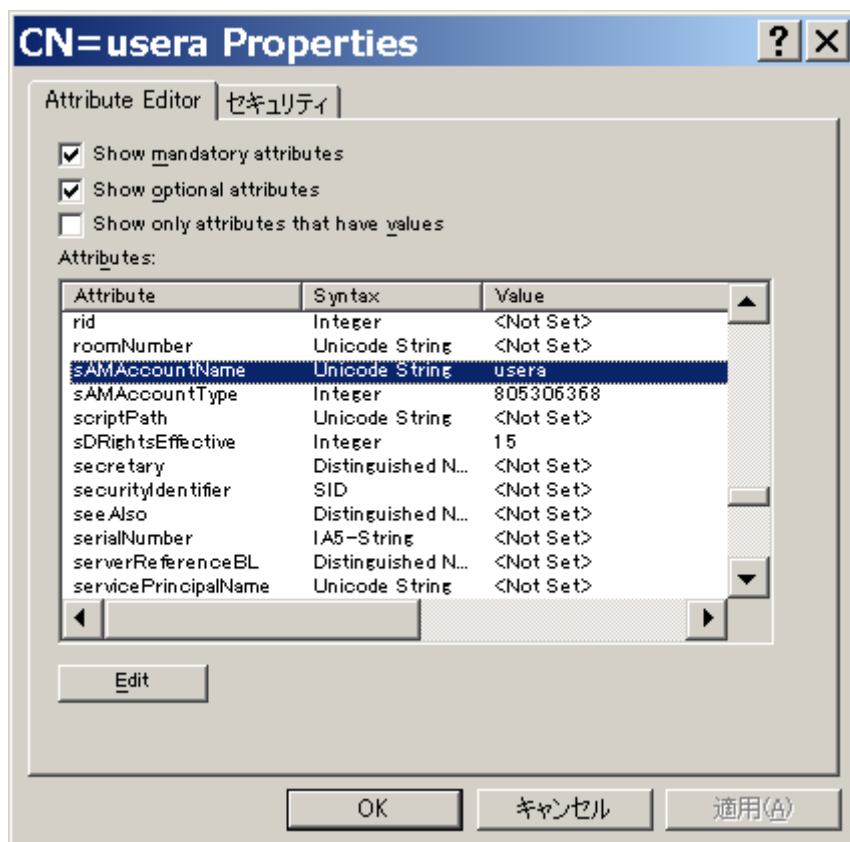
アクセス制御属性　ユーザーおよびグループのアクセス権限を示す属性名を指定します。今回はメモ欄を指定するため ”info” と記載します。

アクセス制御区切り記号
アクセス制御の区切り記号を指定します。”;” と設定します。

記入後、右上の［保存］ボタンをクリックします。

3.36.4.4 Active Directory サポートツールについて

Windows Server 2003 以降、インストール CD または DVD にサポートツールが格納されています。それをインストールすることで、Active Directory の各情報を取得することができます。これを使うと、dc=、cn=、ou=などのパラメーターを確認することができます。
インストールメディアの ¥SUPPORT¥TOOLS ディレクトリにある suptool.msi をインストールしてください。

インストールが終わったら、スタートメニューの「ファイル名を指定して実行」において「mmc」と入力してください。

下のような管理コンソールが開きます。

メニューバーー”ファイル” から、「スナップインの追加と削除」を実行すると下のような「スナップインの追加と削除」ウィンドウが表示されます。「追加」ボタンをクリックします。

下のような「スタンドアロン スナップインの追加」ウィンドウが表示されます。”ADSI Edit”を選択し、「追加」ボタンをクリックします。

「OK」ボタンをクリックし、スナップインの追加を終了します。

管理コンソール画面で、追加した「ADSI Edit」を右クリックし、「Connect to…」を実行します。

下のような「Connection Settings」ウィンドウが表示されます。そのまま「OK」ボタンをクリックします。

Active Directory サーバーのディレクトリ状態が表示されます。
OU=KVM を探し、その下にある demo1 のプロパティを開きます。

下のようなウィンドウが表示されます。

ここに表示されている「Attributes」が検索クエリで参照される各パラメーターを示します。
”sAMAccountName” や ”info” が存在していることが確認できます。

以上で、Active Directory サーバーを用いる方法について説明を終わります。

本装置は LDAP に対応しています。検索とクエリに指定したコンテナやアトリビュート、本装置が LDAP に問い合わせする際のアカウント情報さえ明確であれば、Active Directory ではなく OpenLDAP + Linux を使うことも可能です。

Chapter 4 - ビデオセッションビューア

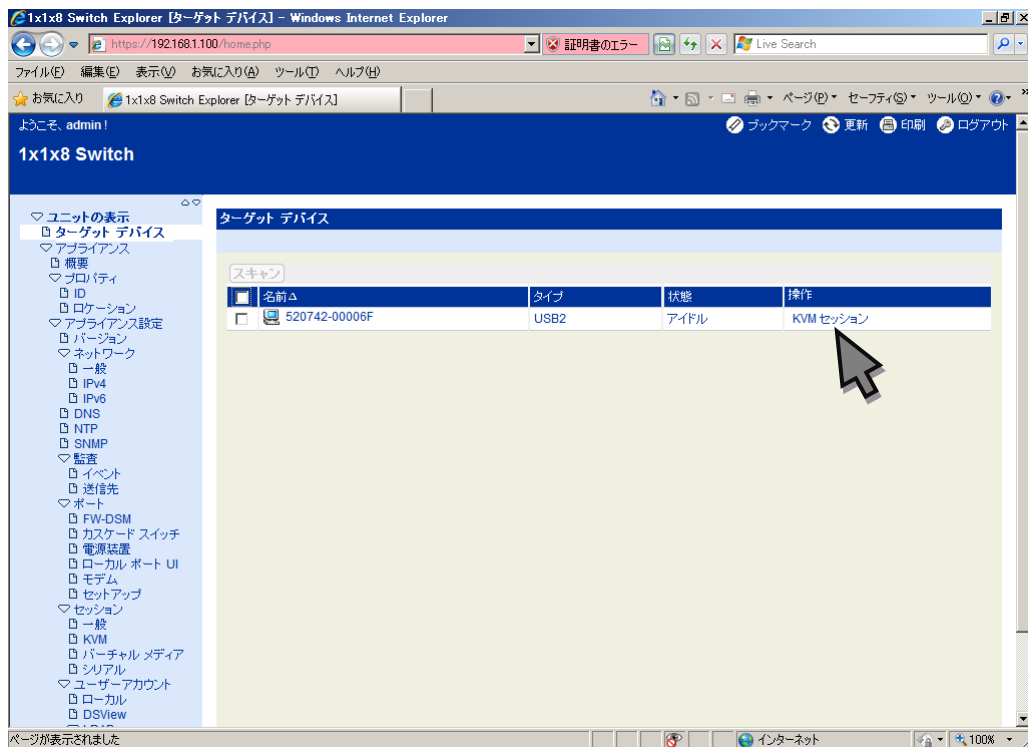
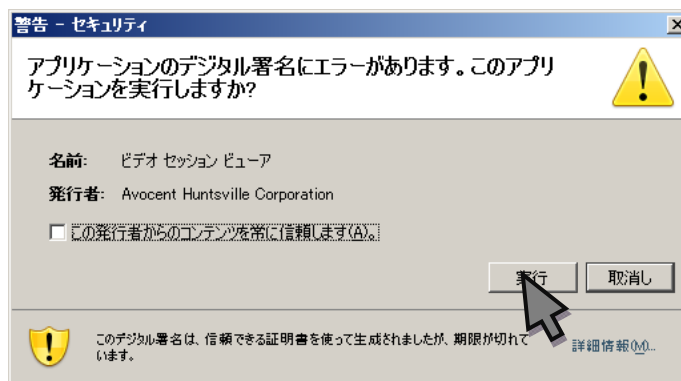
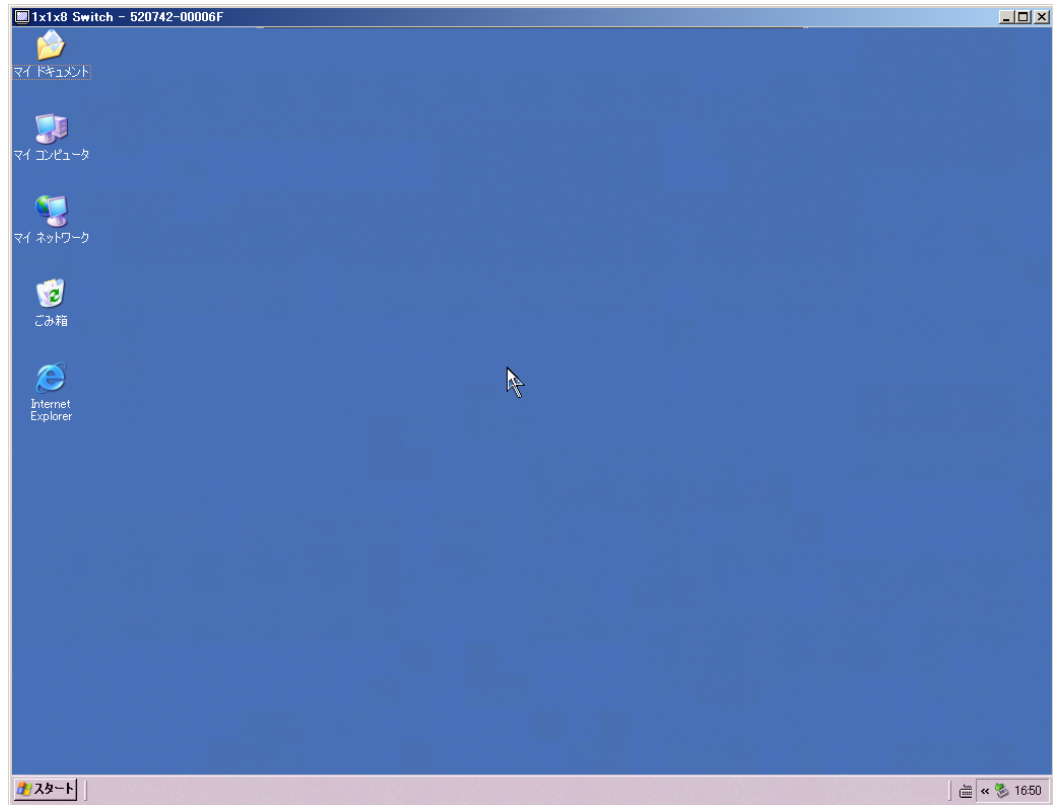
ターゲットデバイスを操作するビデオセッションビューアの使用方法について説明しています。

本章の内容

4.1. ビデオセッションビューアの起動

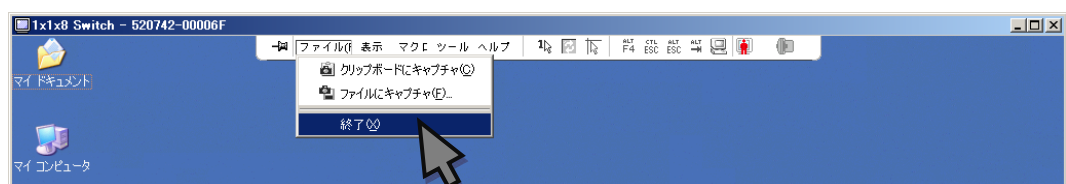
重要

ビデオセッションビューアを起動するには、あらかじめ リモート端末に Java Runtime Environment（JRE）のバージョン 1.6 以降をインストールしておく必要があります。
Java のサイトからダウンロードしてインストールしてください。

OBWI の「ターゲットデバイス」ページにおいて、操作対象のターゲットデバイスの ”KVM セッション” 表示をクリックします。

下のような、警告ダイアログが表示される場合は、「実行」ボタンをクリックします。

下のようなビデオセッションビューア画面が起動し、ターゲットデバイスのデスクトップ画面が表示され、キーボード、マウスの操作が可能となります。この状態のセッションを KVM セッションと呼びます。

通常、ビデオセッションビューアからターゲットデバイスを操作する場合、リモート端末側のマウスカーソルとターゲットデバイスのマウスカーソルの 2 種類が表示されている状態となります。マウスカーソルの動作としては、リモート端末側のカーソル移動にターゲットデバイス側のカーソルがついてくる形になります。

・白色で一回り小さいカーソルが
　ターゲットデバイス側のマウスカーソル
・透明で大きい方のカーソルが
　リモート端末側のマウスカーソル
　（カーソル形状は設定変更可能）

リモート端末側のマウスカーソルの形状を変更する場合は、以下をご参照ください。
📖 参照 4.11.1 マウスカーソルの設定（182 ページ）

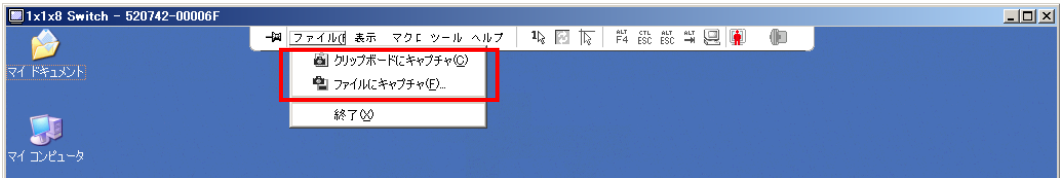
ビデオセッションビューアを終了させる場合は、メニューバーにおいて、"ファイル"－"終了"をクリックするか、ウィンドウの右上の「×」ボタンをクリックします。

ターゲットデバイスからのビデオ信号の入力がない場合、下のように「シグナルなし」という表示になります。電源設定において、アイドル状態で一定期間経過すると、モニターの電源を切る設定になっているような場合にも「シグナルなし」となりますのでご注意ください。

4.2. メニューバーの表示

ビデオセッションビューアにおいて、マウスカーソルを表示領域の上端に移動させるとメニューバーが表示されます。このメニューバーから各種設定を行うことができます。

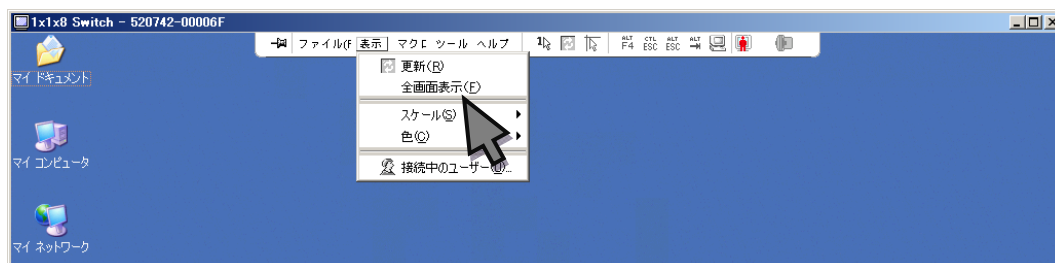
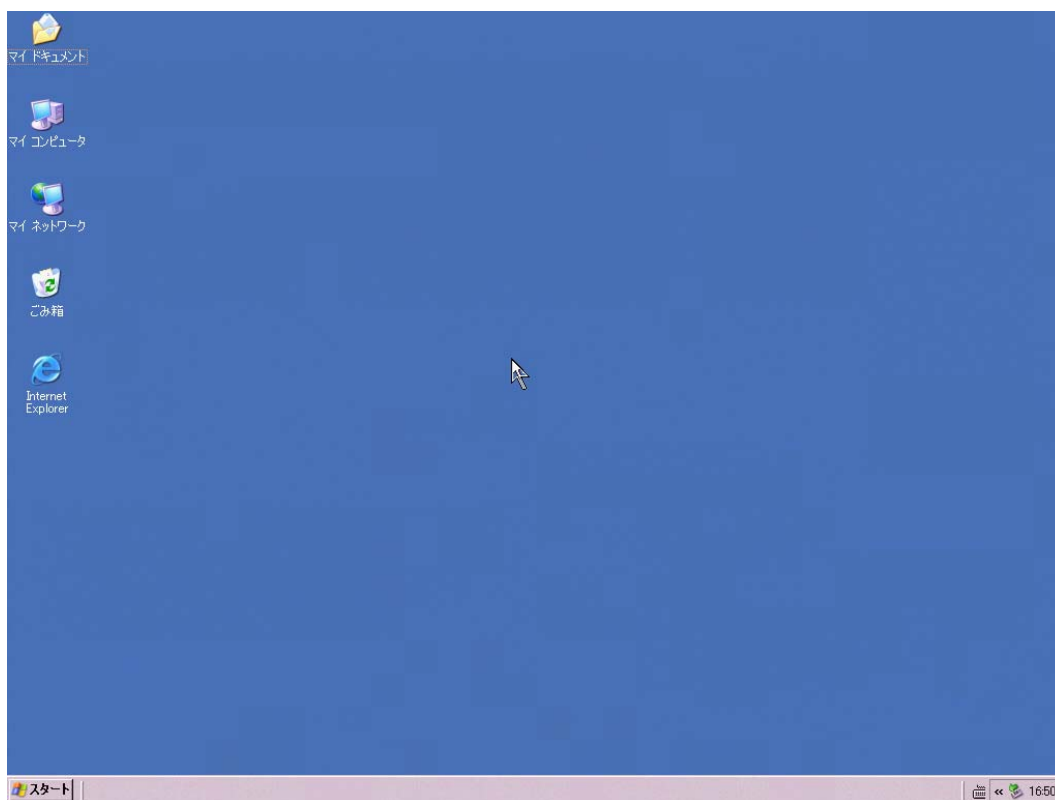
項	表示項目	表示内容
1	ファイル	サーバー表示のキャプチャなどの操作を行います。 📖 参照 4.3 ターゲットデバイス表示のキャプチャ（172 ページ）
2	表示	ウィンドウサイズや色などビデオ表示に関する設定を行います。 📖 参照 4.4 ビデオセッションビューアの全画面表示（173 ページ） 📖 参照 4.5 ビデオセッションビューアのスケール表示（174 ページ） 📖 参照 4.6 ビデオセッションビューアの色設定（175 ページ） 📖 参照 4.7 接続中のユーザーの確認（176 ページ）
3	マクロ	ターゲットデバイスへ入力するマクロキーの設定を行います。 📖 参照 4.8 キーボードマクロの送信（177 ページ）
4	ツール	ビデオ表示など各種設定を行います。 📖 参照 4.9 自動ビデオ調整（179 ページ） 📖 参照 4.10 手動ビデオ調整（180 ページ） 📖 参照 4.11 セッションオプション（181 ページ） 📖 参照 4.12 シングルカーソルモード（189 ページ） 📖 参照 4.13 バーチャルメディア（190 ページ）
5	ヘルプ	ビデオセッションビューアのバージョンを表示します。
6		シングルカーソルモードボタン。 リモート端末側のマウスカーソルを非表示にし、ターゲットデバイス側のカーソルのみを表示させます。 📖 参照 4.13 バーチャルメディア（190 ページ）
7		ビデオ更新ボタンです。 ターゲットデバイスのビデオ表示をリロードします。
8		カーソルの位置合わせボタンです。リモート端末側とターゲットデバイス側のマウスカーソルの位置合わせを実行します。
9	ALT F4	Alt + F4 マクロボタンです。 ターゲットデバイスへ Alt + F4 キーを入力します。
10	CTL ESC	Ctrl + Esc マクロボタンです。 ターゲットデバイスへ Ctrl + Esc キーを入力します。
11	ALT ESC	Alt + Esc マクロボタンです。 ターゲットデバイスへ Alt + Esc キーを入力します。
12	ALT	Alt マクロボタンです。 ターゲットデバイスへ Alt キーを入力します。
13		Ctrl + Alt + Delete マクロボタンです。 ターゲットデバイスへ Ctrl + Alt + Delete キーを入力します。
14		セッションタイプを示すインジケーターです。 📖 参照 4.15 セッションタイプ（199 ページ）

4.3. ターゲットデバイス表示のキャプチャ

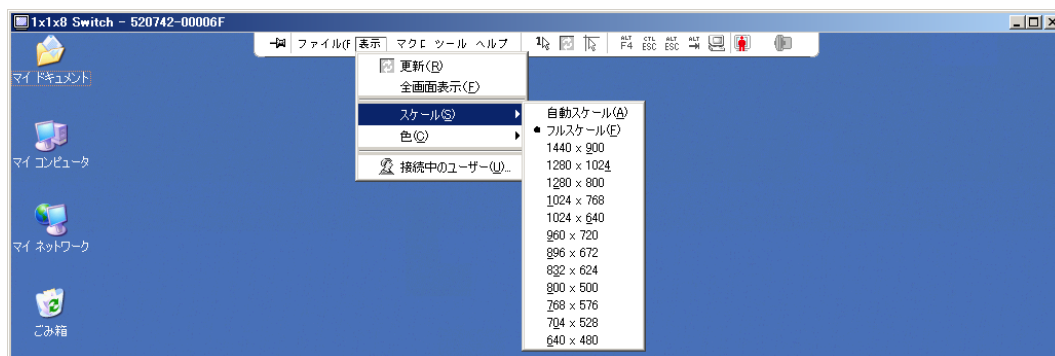
ビデオセッションビューアの メニューバーにおいて、"ファイル" をクリックすると、下のように「クリップボードにキャプチャ」および「ファイルにキャプチャ」という内容が表示されます。本機能は、現在のターゲットデバイスの表示をキャプチャ保存する場合に使用します。

それぞれの機能は、下のとおりです。

項	表示	内容
1	クリップボードにキャプチャ	現在表示されているターゲットデバイスの表示をクリップボードにキャプチャします。
2	ファイルにキャプチャ	現在表示されているターゲットデバイスの表示をキャプチャし、jpeg ファイルとして保存します。

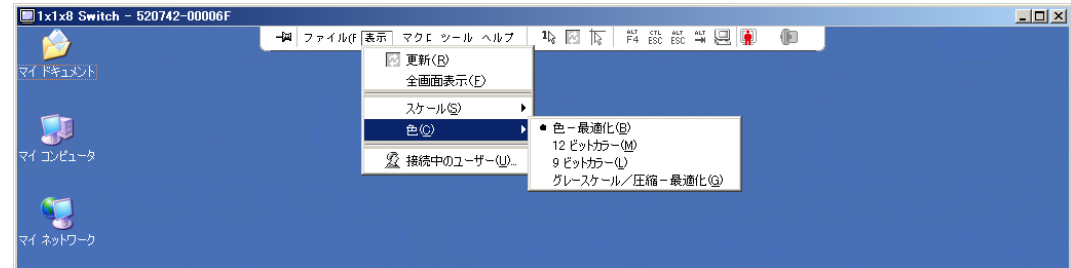
4.4. ビデオセッションビューアの全画面表示

ビデオセッションビューアの メニューバーにおいて、"表示"ー"全画面表示" をクリックすると、リモート端末のデスクトップ上にターゲットデバイスのデスクトップ画面が全画面で表示されます。

下のようにタイトルバーやウィンドウ枠の表示がなくなり、ターゲットデバイスのデスクトップが全画面表示されます。

ただし、ターゲットデバイスの画面解像度がリモート端末の画面解像度よりも低い場合は、ターゲットデバイスのデスクトップ画面の外側は黒色背景として表示されます。

4.5. ビデオセッションビューアのスケール表示

ビデオセッションビューアの メニューバーにおいて、"表示"ー"スケール" をクリックすると、下のようにビデオセッションビューアの表示サイズに関する設定を行うことができます。

「自動スケール」に設定されている場合、リモート端末の画面解像度に合わせて、自動的に全画面をスクロールすることなく表示できるように調整したサイズで表示されます。
「フルスケール」に設定されている場合、ターゲットデバイス側の画面解像度で表示されます。

4.6. ビデオセッションビューアの色設定

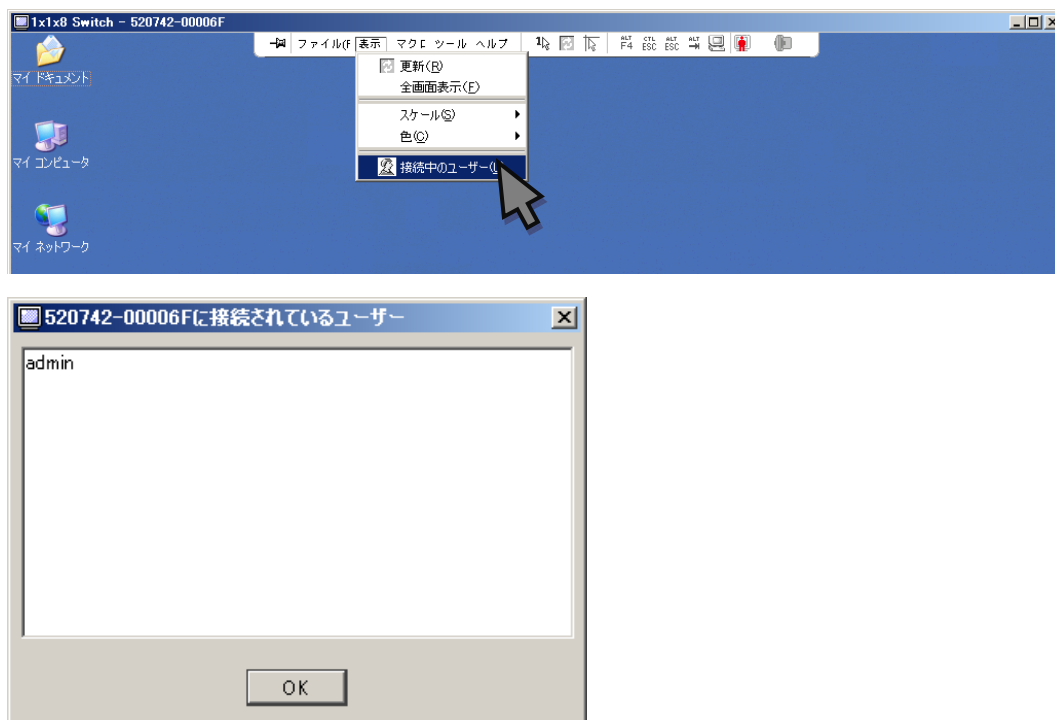
ビデオセッションビューアの メニューバーにおいて、"表示"ー"色" をクリックすると、下のようにビデオデータの色設定を行うことができます。本設定を変更することにより、帯域を制御することができます。

各設定内容は、下のとおりです。

項	表示	内容
1	色－最適化	色設定を 16bit にします。
2	12 ビットカラー	色設定を 12bit にします。
3	9 ビットカラー	色設定を 9bit にします。
4	グレースケール／ 圧縮－最適化	色設定をグレースケールにします。

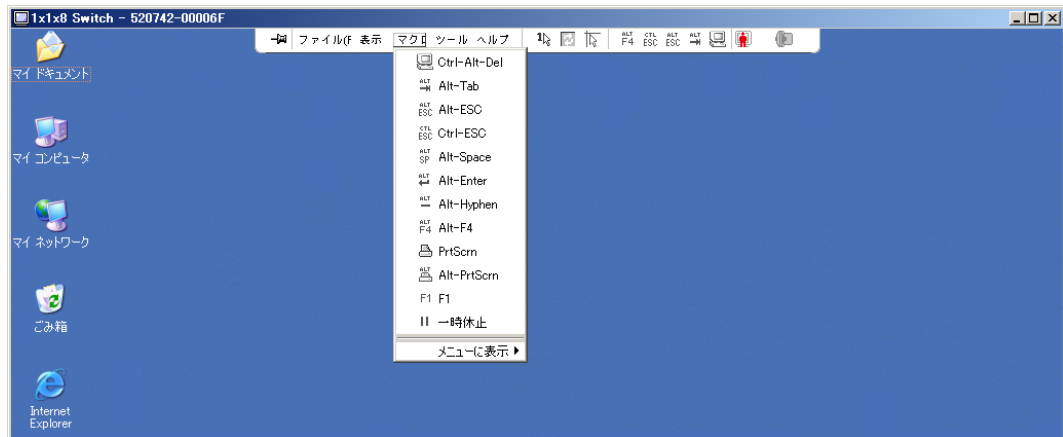
項 1 から 4 の設定へ進むにつれて、画質を抑えることとなりますが、同時にネットワークトラフィックを低減することができます。
マウスカーソルの動作遅延が著しい場合は、色設定を低く変更してください。マウス動作はスムーズになります。

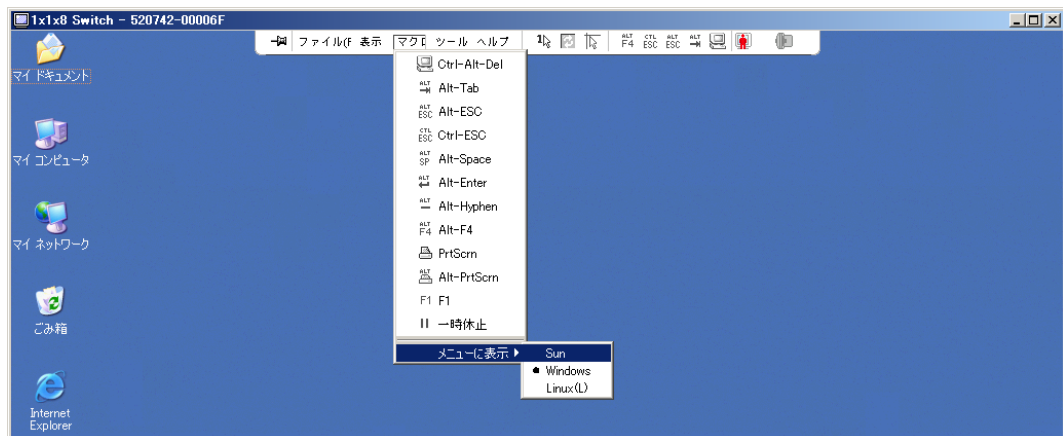
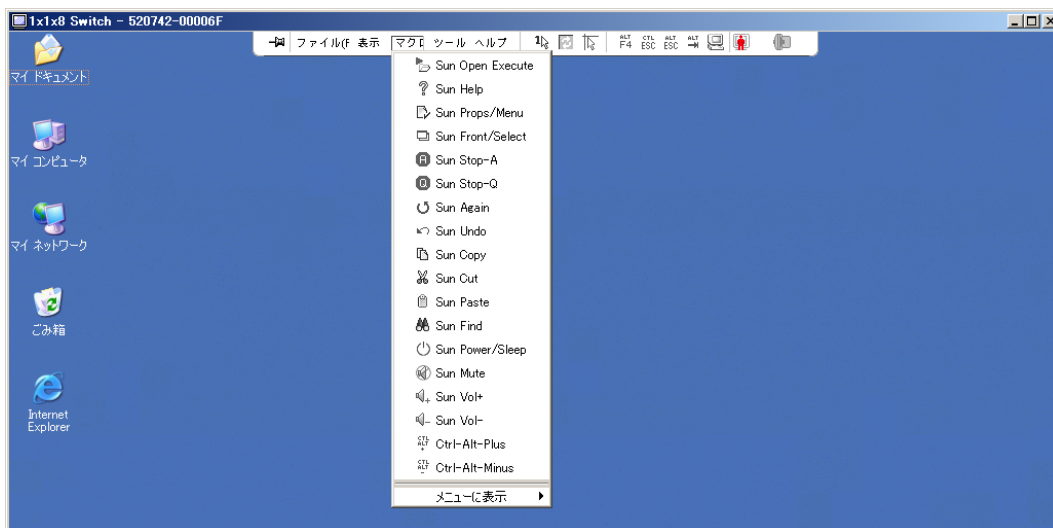
また、本設定はビデオセッションビューアの起動時にネットワークの状況を判別して自動的に設定されます。色設定を "色－最適化" などに上げることができる状態であれば、設定を変更してください。

4.7. 接続中のユーザーの確認

ビデオセッションビューアの メニューバーにおいて、"表示"ー"接続中のユーザー" をクリックすると、下のように現在ビデオセッションビューアに接続しているユーザーを確認することができます。

現在、このターゲットデバイスに接続しているユーザー名称が表示されます。

4.8.　キーボードマクロの送信

ビデオセッションビューアの メニューバーにおいて、”マクロ” をクリックすると、下のように特定のキー入力を行うためのキーボードマクロを指定することができます。任意のマクロを指定することで、そのキーがターゲットデバイスに送信されます。

4.8.1　マクログループの選択

キーボードマクロの設定として、メニューバーの ”マクロ”－”メニューに表示” において ”Sun” あるいは ”Windows” を選択することにより、マクロに表示されるキー内容（マクログループ）が変更されます。

”マクロ”ー”メニューに表示”ー”Sun” を選択すると、下のように Sun のキーボードで入力する特殊キーのマクロが表示されます。この Sun の特殊キーを選択すれば、ターゲットデバイスにそのキーの入力を行うことができます。

また、同様に ”マクロ”ー”メニューに表示”ー”Linux” を選択すると、Linux で入力する特殊キーのマクロが表示されます。

Sun、Windows あるいは Linux マクログループの選択により、表示されるマクロの種類は、下記のとおりです。

Sun マクログループ

項	マクロキー	項	マクロキー	項	マクロキー
1	Sun Open Execute	7	Sun Again	13	Sun Power/Sleep
2	Sun Help	8	Sun Undo	14	Sun Mute
3	Sun Props/Menu	9	Sun Copy	15	Sun Vol+
4	Sun Front/Select	10	Sun Cut	16	Sun Vol-
5	Sun Stop-A	11	Sun Paste	17	Ctrl-Alt-Plus
6	Sun Stop-Q	12	Sun Find	18	Ctrl-Alt-Minus

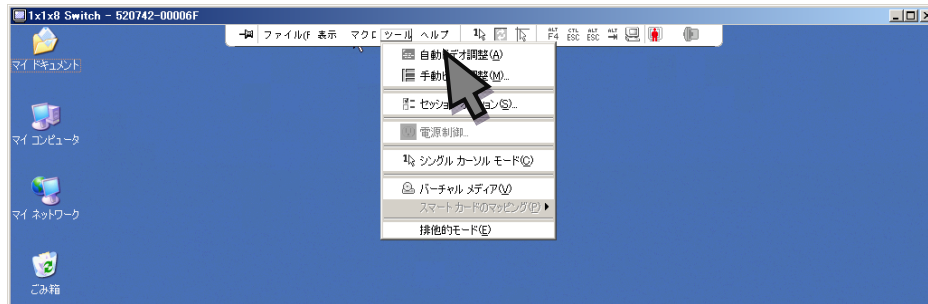
Windows マクログループ

項	マクロキー	項	マクロキー	項	マクロキー
1	Ctrl-Alt-Del	5	Alt-Space	9	PrtScrn
2	Alt-Tab	6	Alt-Enter	10	Alt-PrtScrn
3	Alt-ESC	7	Alt-Hyphen	11	F1
4	Ctrl-ESC	8	Alt-F4	12	一時休止(Pause)

Linux マクログループ

項	マクロキー	項	マクロキー	項	マクロキー
1	Ctrl-Alt-F1	6	Ctrl-Alt-F6	11	Ctrl-Alt-F11
2	Ctrl-Alt-F2	7	Ctrl-Alt-F7	12	Ctrl-Alt-F12
3	Ctrl-Alt-F3	8	Ctrl-Alt-F8	13	Ctrl-Alt-Esc
4	Ctrl-Alt-F4	9	Ctrl-Alt-F9	14	Ctrl-Alt-Backspace
5	Ctrl-Alt-F5	10	Ctrl-Alt-F10		

4.9. 自動ビデオ調整

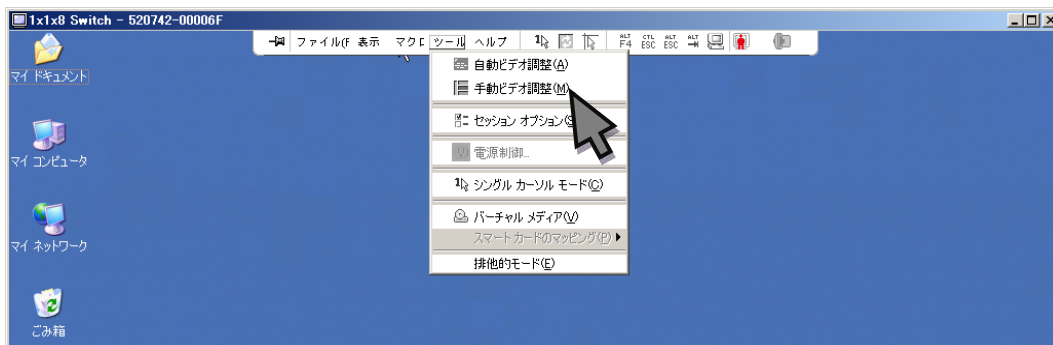
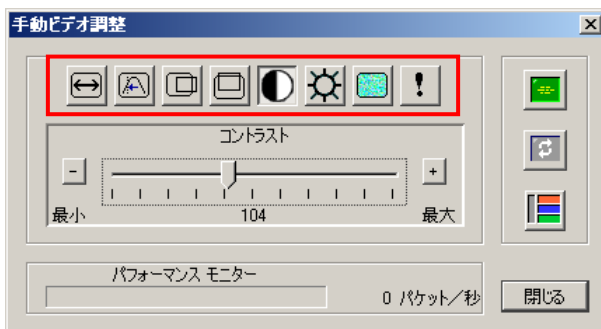
ビデオセッションビューアの メニューバーにおいて、”ツール”－”自動ビデオ調整” をクリックすると、ターゲットデバイスのビデオ表示を自動的に調整させることができます。
表示位置、明るさなどのパラメーターを最適化し、色のにじみ、チラつきなどがある場合には、ビデオ表示を調整可能な範囲で改善することができます。

自動調整の間、下のように「較正中」と表示されます。約 5～10 秒で調整は終了し、ターゲットデバイスの表示に戻ります。

画質に問題があると感じたり、表示位置がずれている場合は、自動ビデオ調整を実行してください。

重要

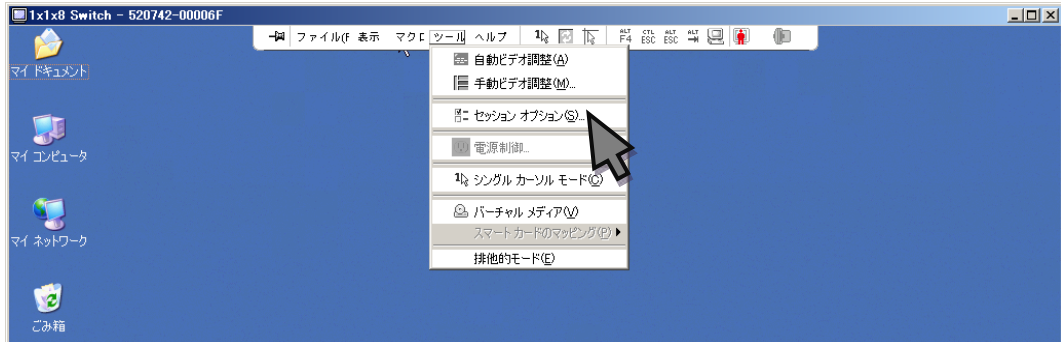
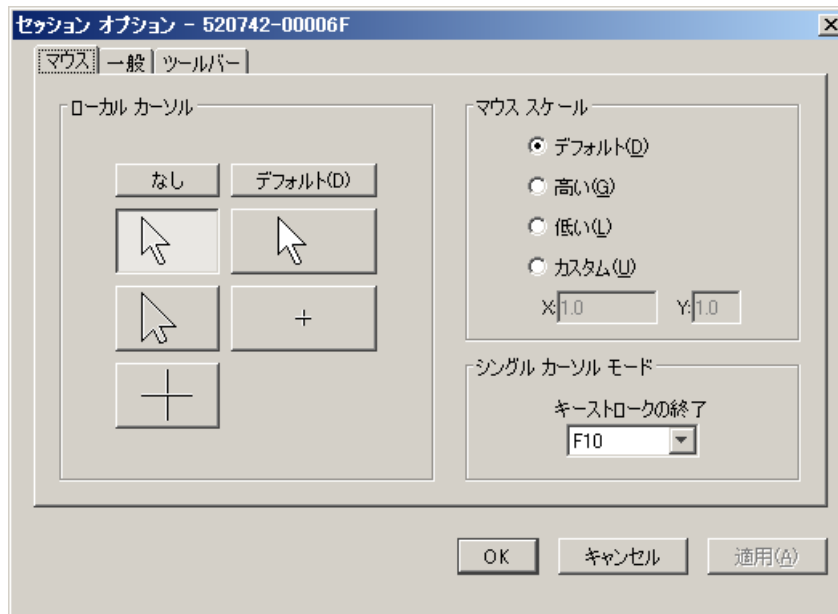
本製品では校正ではなく較正を使っております。 ビデオ信号の調整に掛かるものとして電波法の第二十四条の二や JIS Z 8103 に基づき、「調整した設定値が保存される作業」としての「較正」を使っております。

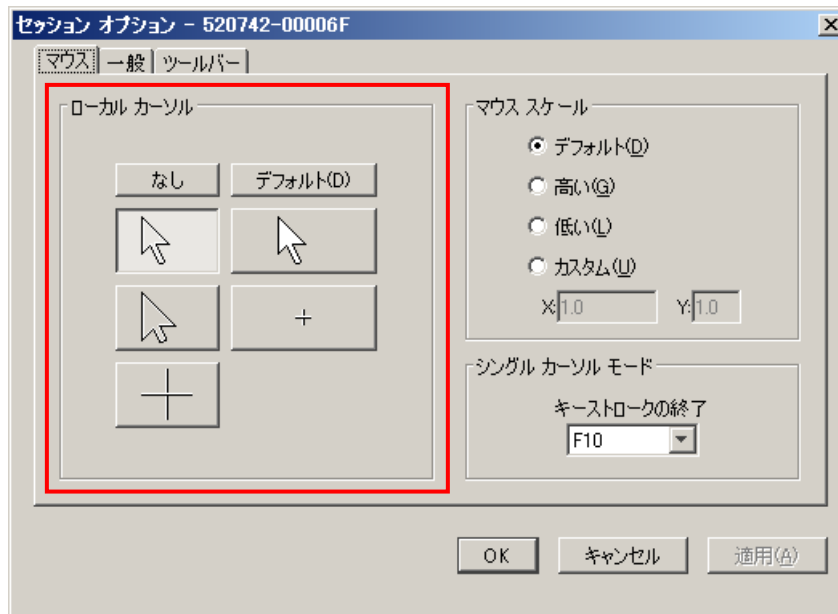
4.10. 手動ビデオ調整

ビデオセッションビューアの メニューバーにおいて、"ツール"ー"手動ビデオ調整" をクリックすると、ビデオ表示に関する各種パラメーターを手動で調整することができます。

下のような、「手動ビデオ調整」ウィンドウが表示されます。
赤枠内の調整パラメータボタンをクリックし、下のスライドバーで値を調整します。

各表示ボタンの内容は、下のとおりです。

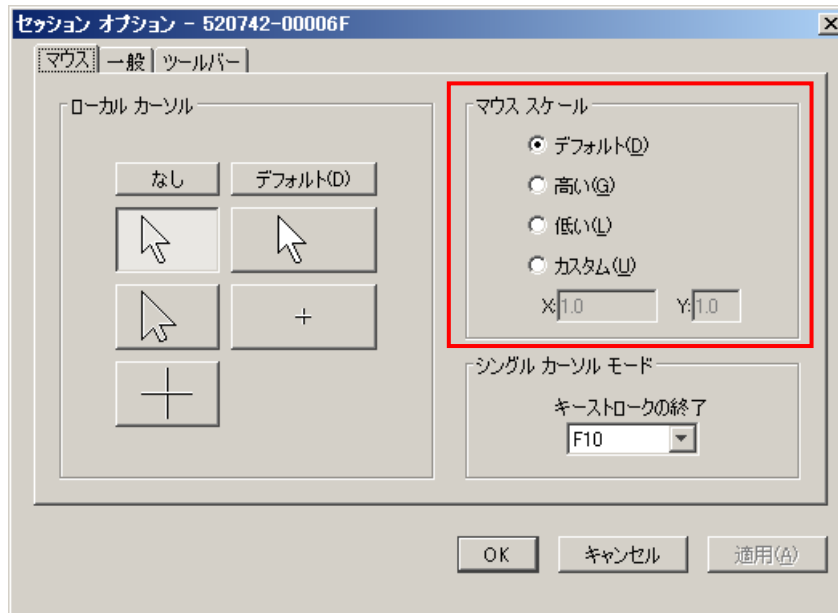
ボタン	設定名称	内容
	画像キャプチャの幅	表示画面の幅を広くしたり、狭くしたりします。
	ピクセルサンプリング微調整	ピクセルサンプリング値を調整します。
	画像キャプチャの水平位置	表示画面の水平位置を左右に調整します。
	画像キャプチャの垂直位置	表示画面の垂直位置を上下に調整します。
	コントラスト	コントラストの大小を調整します。
	明るさ	明るさの大小を調整します。
	ブロックノイズしきい値	ブロックノイズに対するしきい値を調整します。
	ピクセルノイズしきい値	ピクセルノイズに対するしきい値を調整します。
	自動ビデオ調整	上記の全てのパラメーターを自動調整します。
	イメージの更新	ビデオ表示をリロードします。
	ビデオテストパターン	テストパターンを表示します。「手動ビデオ調整」ウィンドウを閉じると、テストパターン表示も終了します。
	パフォーマンスモニター	現在の画面表示に対するネットワークトラフィックの値を表示します。 パケット／秒の単位で表示します。

4.11. セッションオプション

ビデオセッションビューアの メニューバーにおいて、"ツール"－"セッションオプション" をクリックすると、セッションに関する各種設定を行うことができます。

下のような、「セッションオプション」ウィンドウが表示されます。"マウス"、"一般"、"ツールバー" の 3 種類のタブで区切られており、各種オプション設定が可能です。

4.11.1 マウスカーソルの設定

「セッションオプション」ウィンドウの "マウス" タブにおいて、マウスカーソルの表示オプションについて選択することができます。
下のように「ローカルカーソル」領域内に表示された任意のボタンをクリックします。
"なし" を選択すると、リモート端末側のマウスカーソルは、ビデオセッションビューアのウィンドウ画面の枠内にある状態では、非表示となります。
"デフォルト" を選択すると、Windows の標準カーソルの表示となります。変更後、「適用」ボタンをクリックすると反映されます。

4.11.2 マウススケールの設定

「セッションオプション」ウィンドウの ”マウス” タブにおいて、マウスカーソルの加速度動作について設定を行うことができます。
通常、ターゲットデバイスのマウス加速度の設定は、無効にしてご使用いただくこととなりますが、どうしてもマウス加速度を無効にすることができない場合に本項目を調整していただくことでリモート端末側とターゲットデバイス側のマウスカーソルを一致させます。

下のように「マウススケール」領域内で設定を行います。

各設定内容は、下のとおりです。

”デフォルト” リモート端末のマウス動作とターゲットデバイスのマウス動作が 1:1 になります。

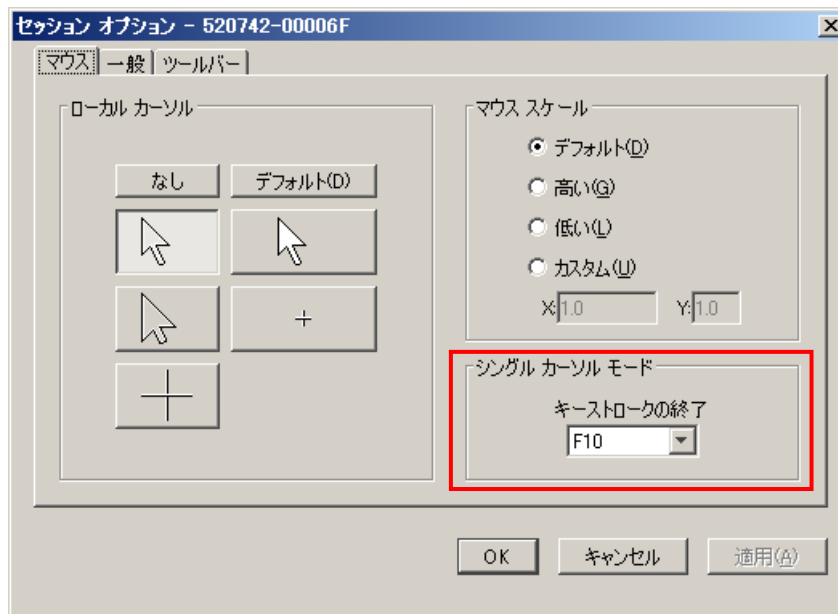
”高い” リモート端末のマウス動作とターゲットデバイスのマウス動作が 1:2 になります。ターゲットデバイス側に 2 倍の動作として伝わります。

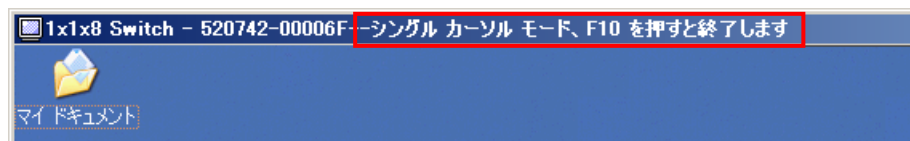
”低い” リモート端末のマウス動作とターゲットデバイスのマウス動作が 1:0.5 になります。ターゲットデバイス側に 1/2 の動作として伝わります。

”カスタム” リモート端末のマウス動作とターゲットデバイスのマウス動作について、任意の割合を指定することができます。有効な入力値の範囲は、0.25～3.00 です。

4.11.3 シングルカーソルモードの終了ホットキーの設定

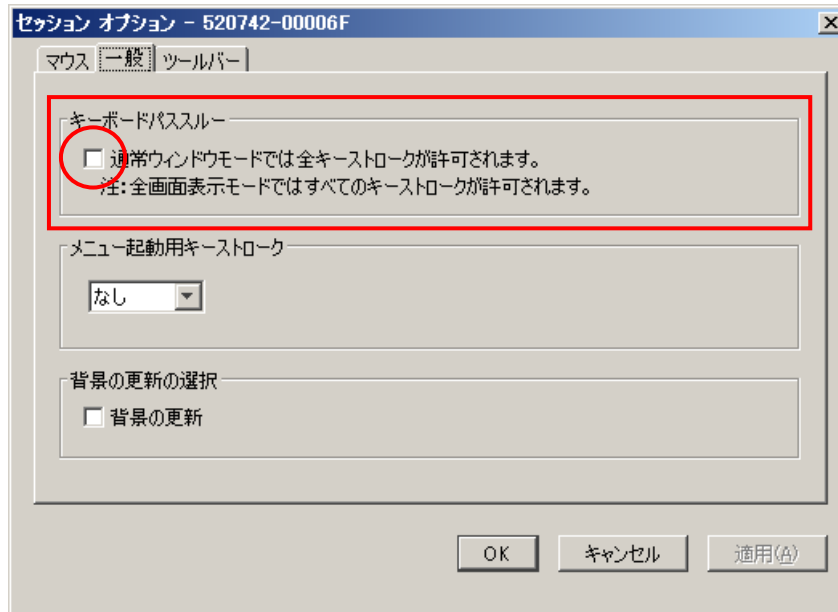
「セッションオプション」ウィンドウの ”マウス” タブにおいて、シングルカーソルモードを終了させ、通常のカーソルモード（リモート端末側のマウスカーソルを表示させる）に戻す際に入力するホットキーの設定を行うことができます。

下のように「シングルカーソルモード」領域内で設定を行います。

”キーストロークの終了” ドロップダウンメニューから任意のキーを選択します。デフォルトで ”F10” キーが選択されています。ドロップダウンメニュー内の ”一時休止” は、Pause キーを意味します。

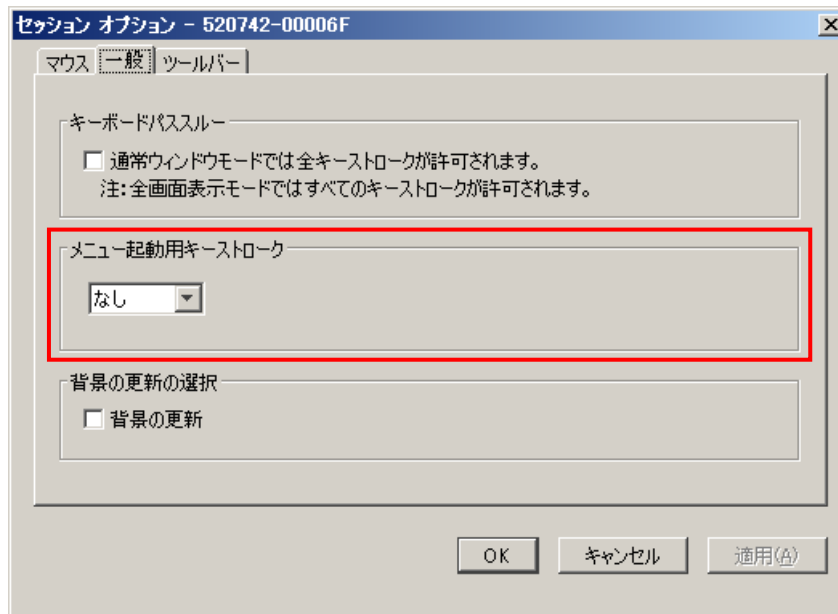
シングルカーソルモードを実行中、タイトルバーに終了ホットキーが表示されます。

シングルカーソルモードの詳細については、以下をご参照ください。

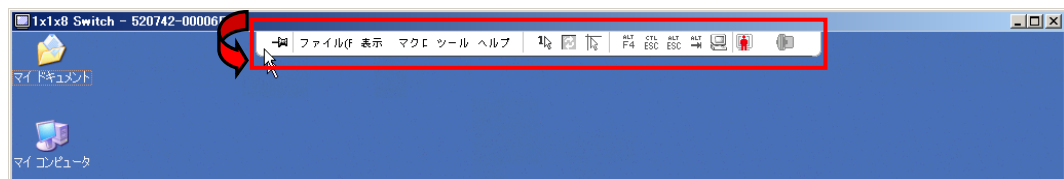
参照 4.12 シングルカーソルモード（189 ページ）

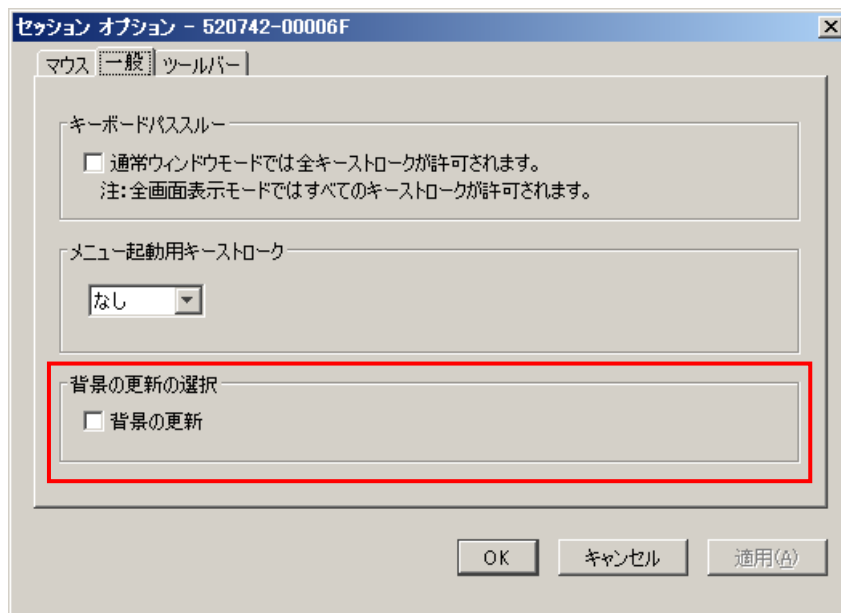
4.11.4 キーボードパススルーの設定

「セッションオプション」ウィンドウの ”一般” タブにおいて、キーボードパススルーの有効／無効の設定を行うことができます。
キーボードパススルーとは、”Ctrl-Alt-Delete” キー以外の全てのリモート端末からのキー入力を直接ターゲットデバイスに送信する動作モードです。（例えば、Windows キーを入力した場合、リモート端末側に入力が伝わることなく、直接ターゲットデバイス側に Windows キーが入力されます。）

”通常ウィンドウモードでは全キーストロークが許可されます” にチェックを入れ、右下の「適用」ボタンをクリックすると キーボードパススルーは、有効となります。本設定は、デフォルトでは無効となっています。

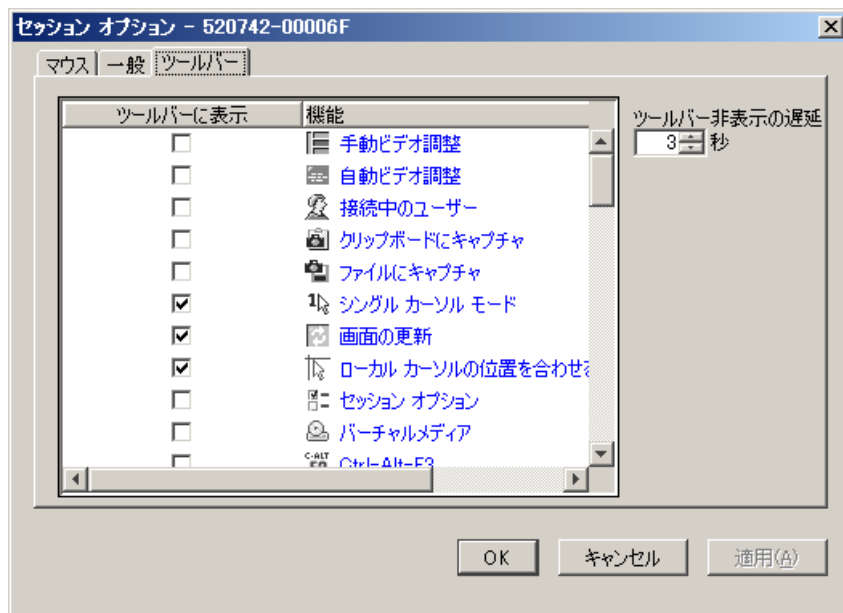
4.11.5 メニューバー表示用ホットキーの設定

「セッションオプション」ウィンドウの ”一般” タブにおいて、ビデオセッションビューアのメニューバーを表示するためのホットキーを設定することができます。

”メニュー起動用キーストローク” ドロップダウンメニューから任意のキーを選択します。
ドロップダウンメニュー内の ”一時停止” は、Pause キーを意味します。
本設定は、デフォルトでは ”なし” となっており、ホットキーは無効の状態です。

例えば、”F1” を選択すると、ビデオセッションビューア画面がアクティブな状態で F1 キーを入力すると、下のようにメニューバーが表示されます。

4.11.6 ビデオデータ送信の設定

「セッションオプション」ウィンドウの ”一般” タブにおいて、ターゲットデバイスからのビデオデータ送信に関する設定を行うことができます。

”背景の更新” にチェックを入れると ターゲットデバイスからのビデオデータを本装置は、連続的に送信します。
”背景の更新” にチェックが入っていない場合、ターゲットデバイスで変化が生じた時のみ本装置は、ビデオデータを送信します。
本設定は、デフォルトでは チェックは入っていません。

4.11.7 ツールバー表示の設定

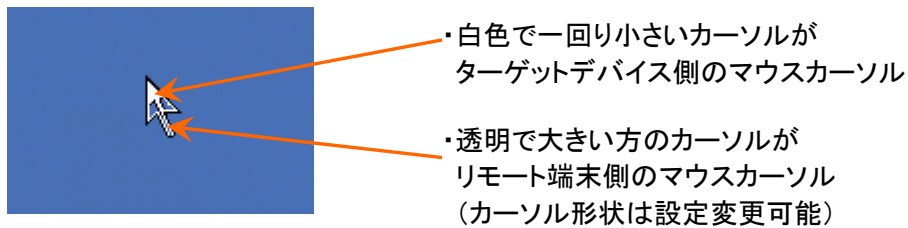
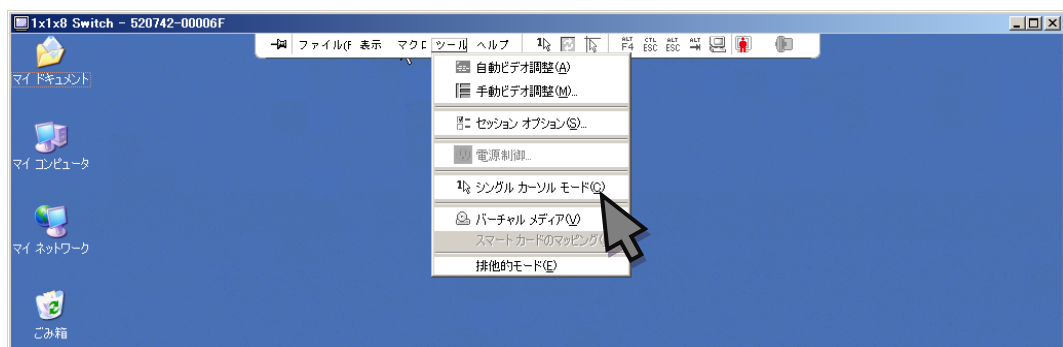
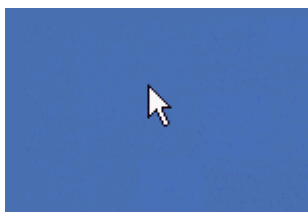
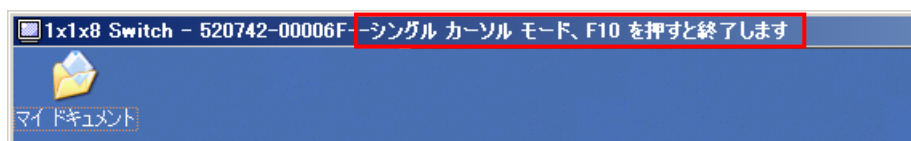
「セッションオプション」ウィンドウの ”ツールバー” タブにおいて、ビデオセッションビューアのツールバーにボタン表示させる項目を設定することができます。
下のように、ツールバーにボタンとして表示させる項目にチェックを入れます。最大 10 個まで選択することができます。

デフォルトで下記の 8 種類にチェックが入っており、ツールバーにボタン表示されています。

- シングルカーソルモード
- 画面の更新
- ローカルカーソルの位置を合わせる
- Alt-F4
- Ctrl-ESC
- Alt-ESC
- Alt-Tab
- Ctrl-Alt-Del

各ボタンの機能については、以下をご参照ください。
📖 参照 4.2 メニューバーの表示（171 ページ）

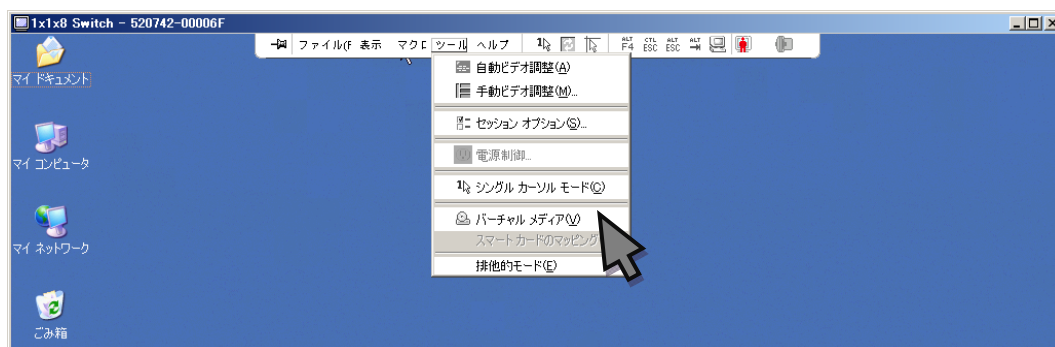
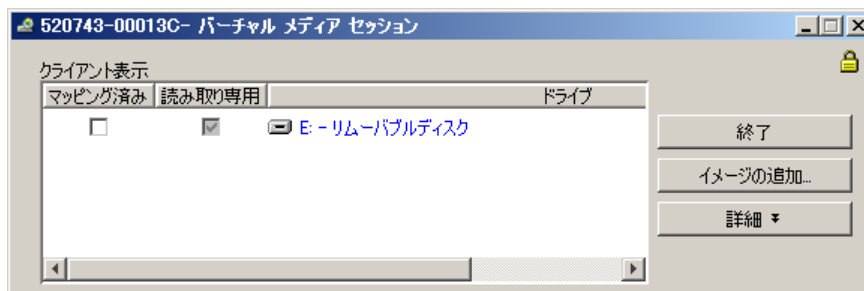
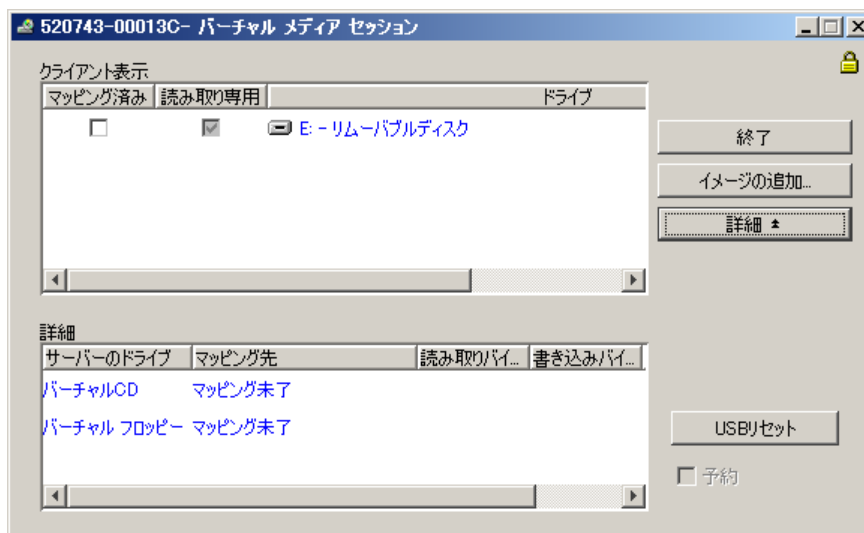
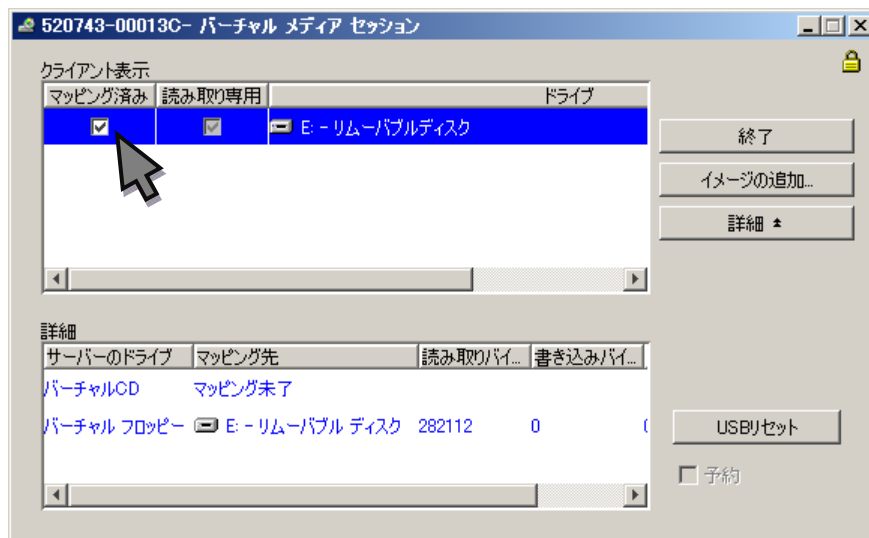
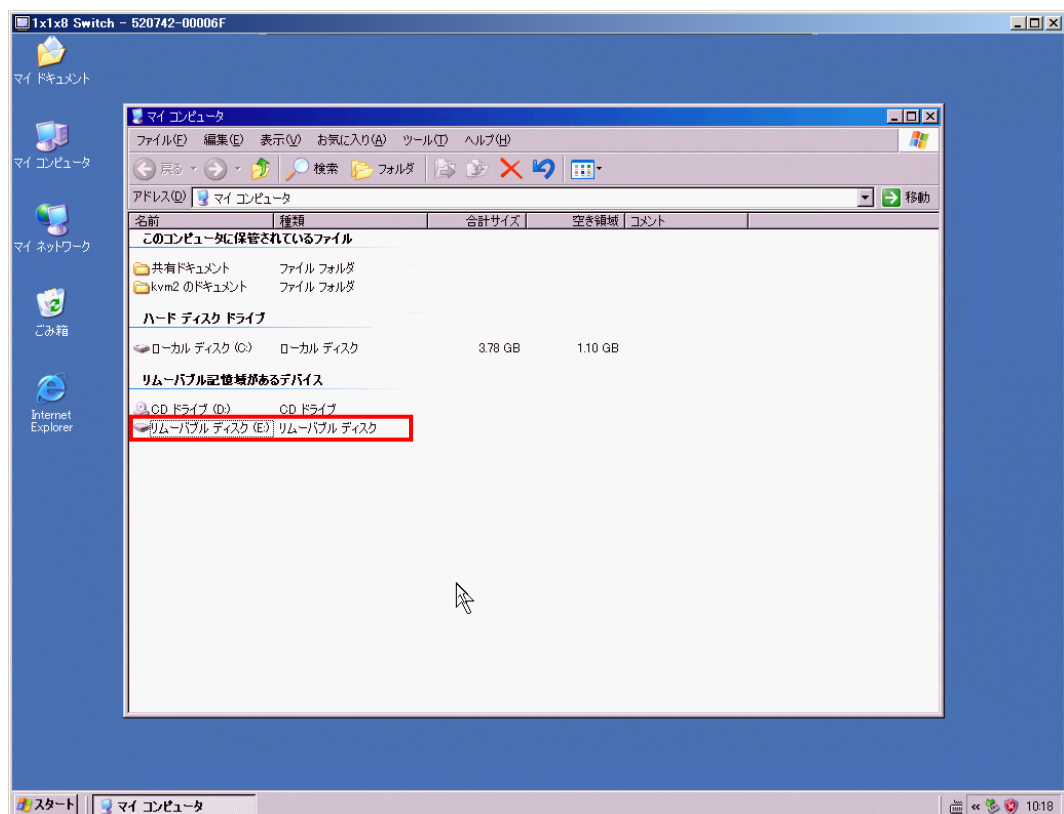
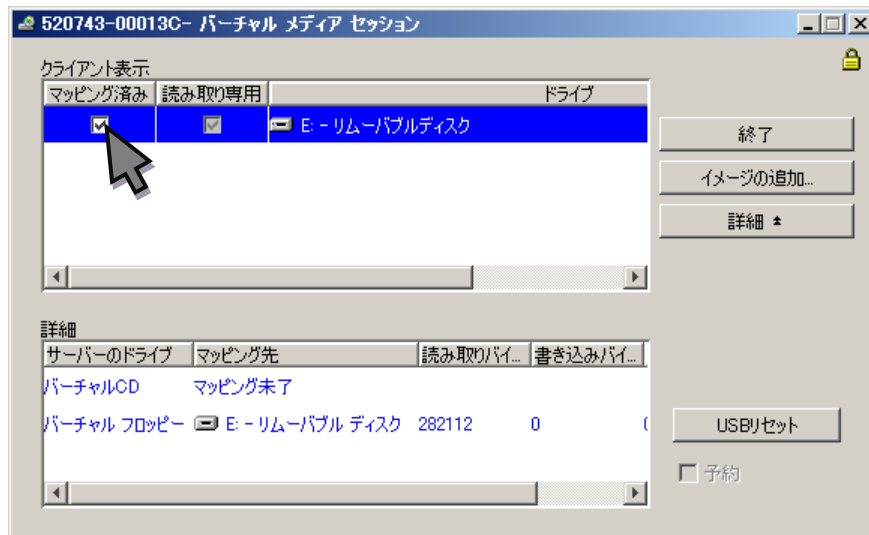
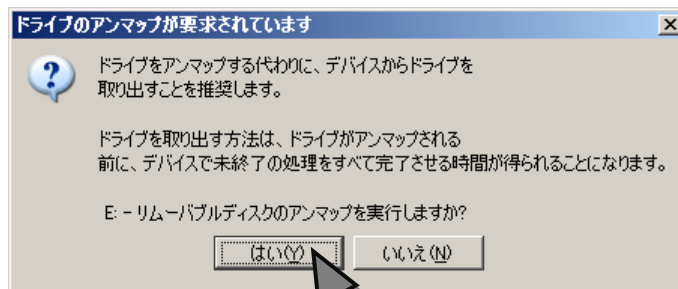
右上の ”ツールバー非表示の遅延” は、ツールバーが表示状態から自動的に隠れる（非表示になる）までの時間設定です。1～10 秒に設定することができます。
デフォルトでは、3 秒に設定されています。

4.12. シングルカーソルモード

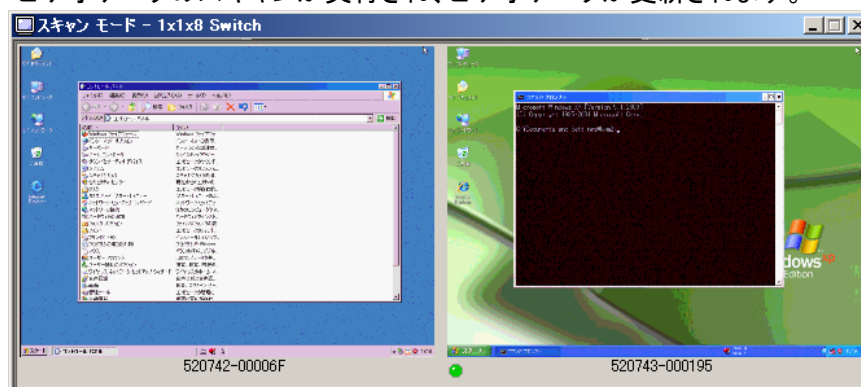
通常ビデオセッションビューアからターゲットデバイスを操作する場合、リモート端末側のマウスカーソルとターゲットデバイスのマウスカーソルが両方表示されている状態となります。マウスカーソルの動作としては、リモート端末側のカーソル移動にターゲットデバイス側のカーソルがついてくる形になります。

ビデオセッションビューアの メニューバーにおいて、"ツール"－"シングルカーソルモード"をクリックすると、ターゲットデバイス側のマウスカーソルのみを表示させることができます。

下のように表示され、リモート端末側のカーソルは表示されません。

シングルカーソルモードを終了させる場合は、下のようにタイトルバーに表示されたホットキーを入力します。デフォルトで F10 キーに設定されています。ホットキーの設定は、セッションオプションの設定で変更することができます。

4.13. バーチャルメディア

バーチャルメディア機能とは、リモート端末からのターゲットデバイスの操作において、リモート端末上に接続されたフロッピーディスク、CD/DVD-ROM、USB ストレージがあたかもターゲットデバイスに直接接続されているかのように、ターゲットデバイスにマッピングさせることができるものです。

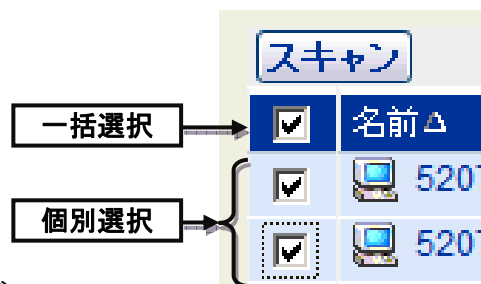
📖 参照 1.5 バーチャルメディア機能（10 ページ）

ビデオセッションビューアの メニューバーにおいて、”ツール”ー”バーチャルメディア” をクリックすると、バーチャルメディア機能に関する設定を行うことができます。

下のような「バーチャルメディアセッション」ウィンドウが表示されます。
このウィンドウには、リモート端末のドライブ情報が表示されます。ここでは、リモート端末にリムーバブルディスクが接続されていることを示しています。

「詳細」ボタンをクリックすると、下のようにバーチャルメディアのマッピング状況を確認することができます。

ターゲットデバイスに対してバーチャルメディアを認識させるには、ドライブ表示の左側にある "マッピング済み" チェックボックスにチェックを入れます。

バーチャルメディアのマッピングが実行され、この場合は、ターゲットデバイス側のリムーバブルディスクにアクセスが可能となります。

ターゲットデバイスからバーチャルメディアを取り外す(アンマップ)する場合は、「バーチャルメディアセッション」ウィンドウで ”マッピング済み” チェックボックスのチェックを外します。

下のような確認ダイアログが表示されます。「はい」ボタンをクリックします。

4.14. スキャンモード

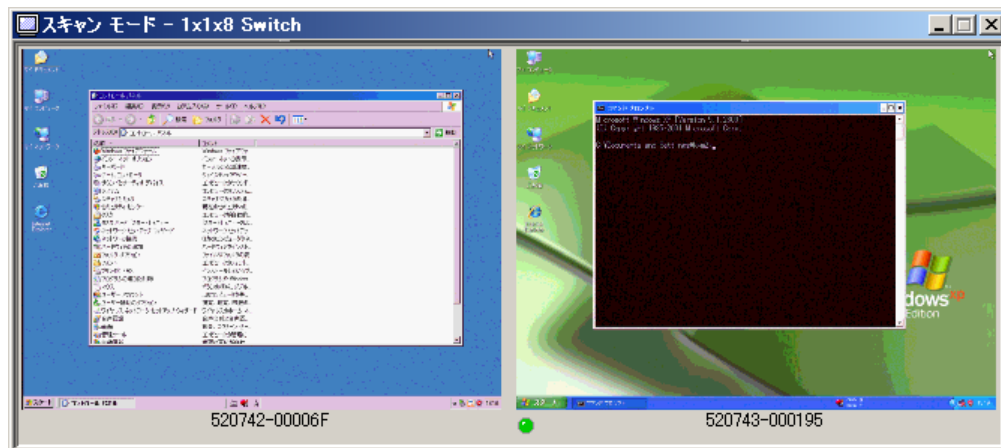
OBWI からのスキャンモードでは、複数のターゲットデバイスをサムネイルビューアで表示させることができ、1 台ずつ順番にターゲットデバイスのビデオデータを更新する監視動作を実行します。その際、キーボードおよびマウス操作はできません。
画面左のメニュー選択領域において、「ユニットの表示」-「ターゲットデバイス」をクリックすると下のような「ターゲットデバイス」ページが表示されます。
スキャンするターゲットデバイスのチェックボックスにチェックを入れ、「スキャン」ボタンをクリックします。最大 16 台までのターゲットデバイスをスキャンモードで参照することができます。

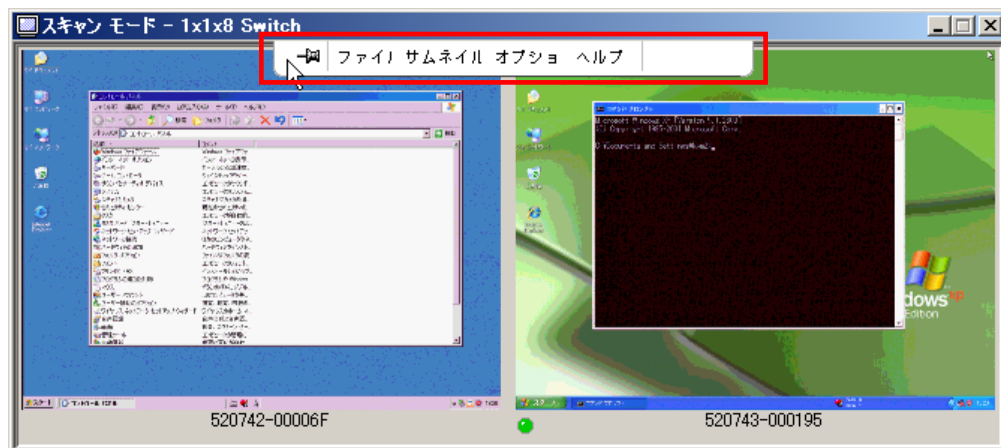
下のような、スキャンモードのビデオビューア画面が表示され、ターゲットデバイス 1 台毎にビデオデータのスキャンが実行され、ビデオデータが更新されます。

スキャンを行っているターゲットデバイスに対しては、キーボードおよびマウス操作はできませんが、スキャンの間は接続状態となります。
また、同時接続ユーザー数を超える状態でスキャンを行うことはできません。
例えば、FW-D1108NP の場合、リモートからの同時接続ユーザー数は 1 であるため、他のユーザーがビデオセッションビューアを実行している間は、スキャンモードを実行してもスキャンすることはできず、失敗となります。

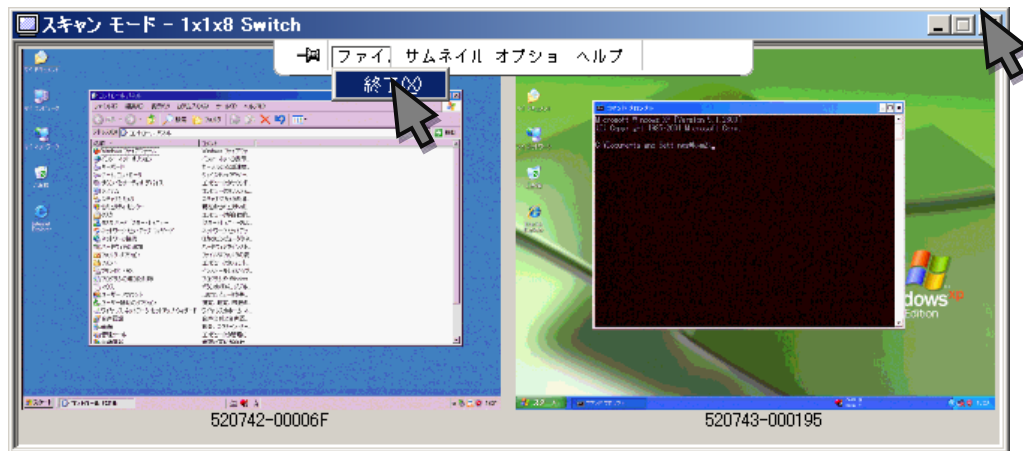
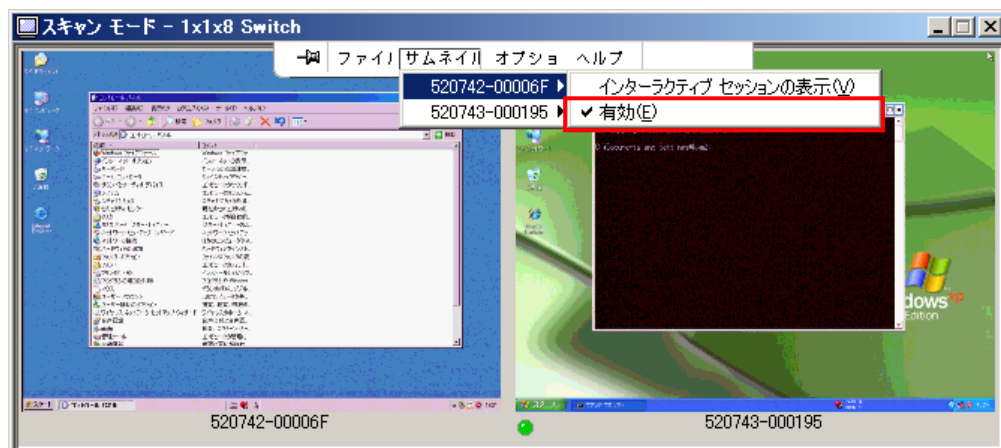
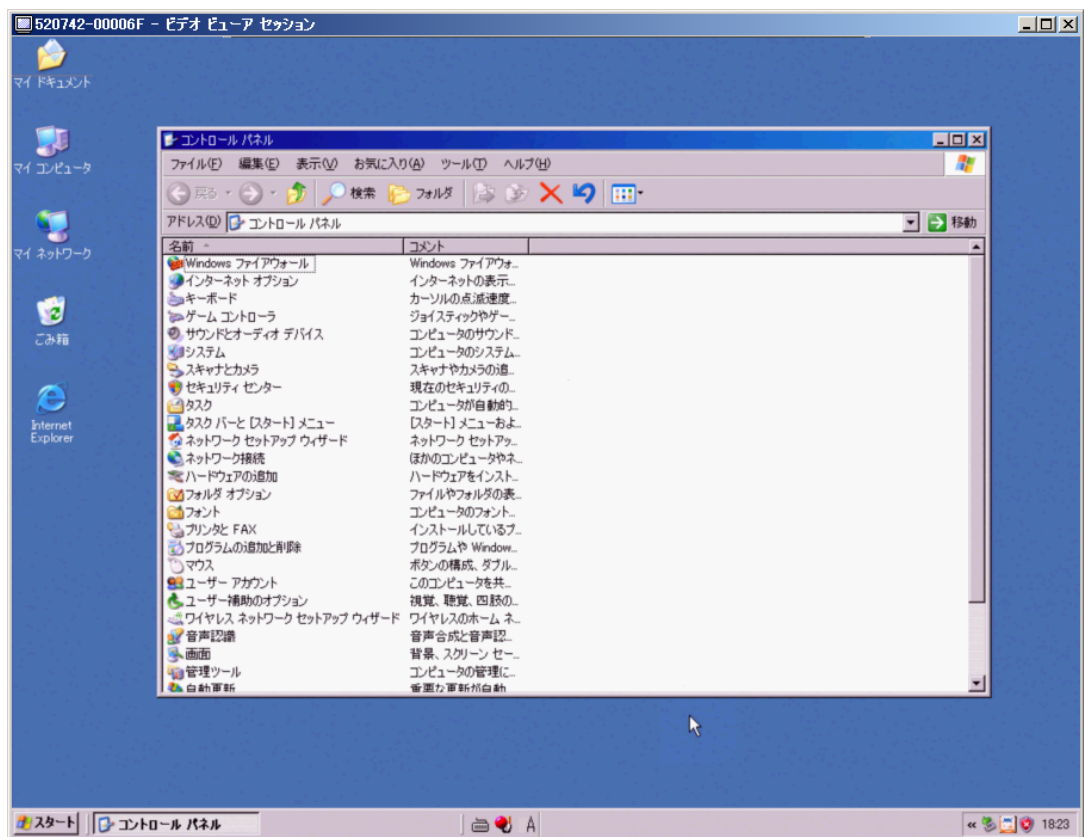
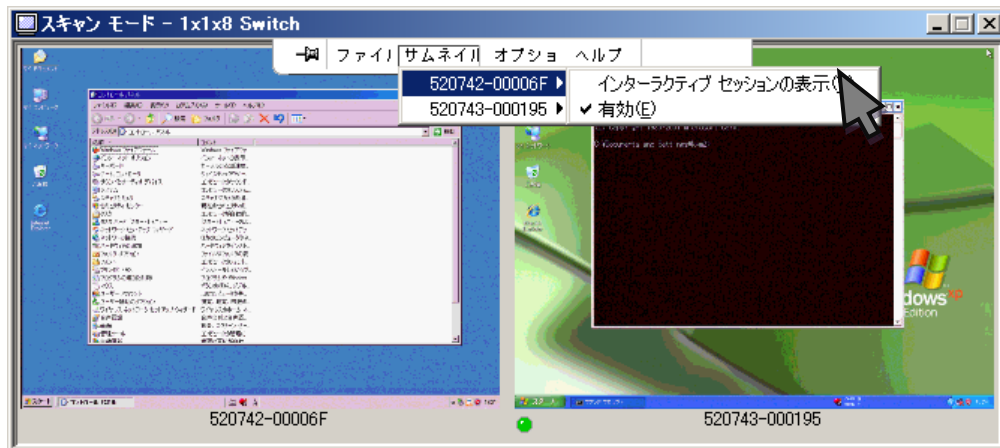
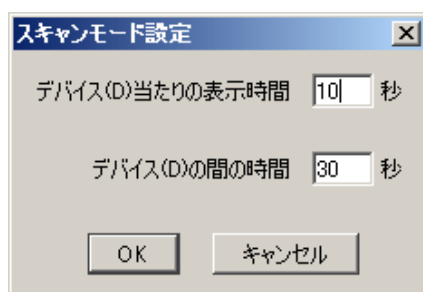
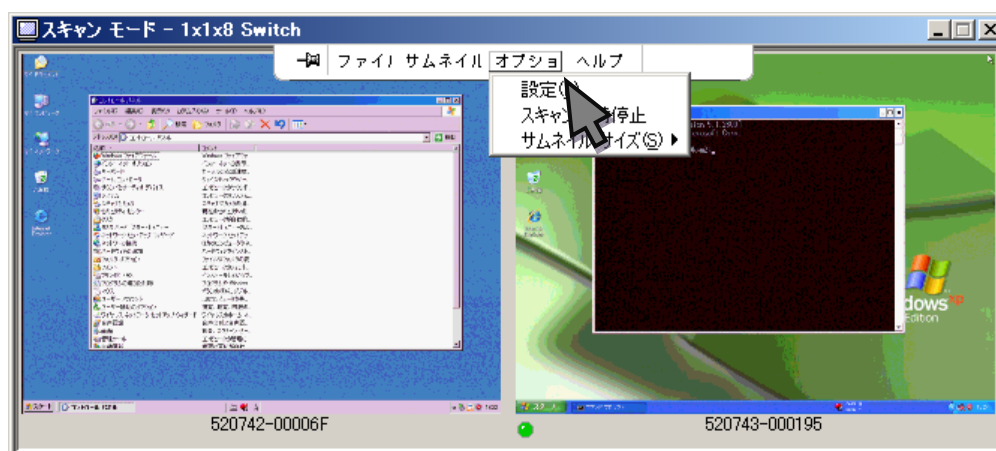
重要（スキャン順）

予めスキャン順を決める方法があります。 右図において、一括選択にチェックを入れると、スキャン順は名前順なります。
個別選択にて一つ一つチェックしていく場合、チェックした順にスキャンが行われます。

4.14 スキャンモード

各フレームの画面表示の下にサーバー名称と状態を示すインジケーターが表示されます。
インジケーターの内容は、下のとおりです。

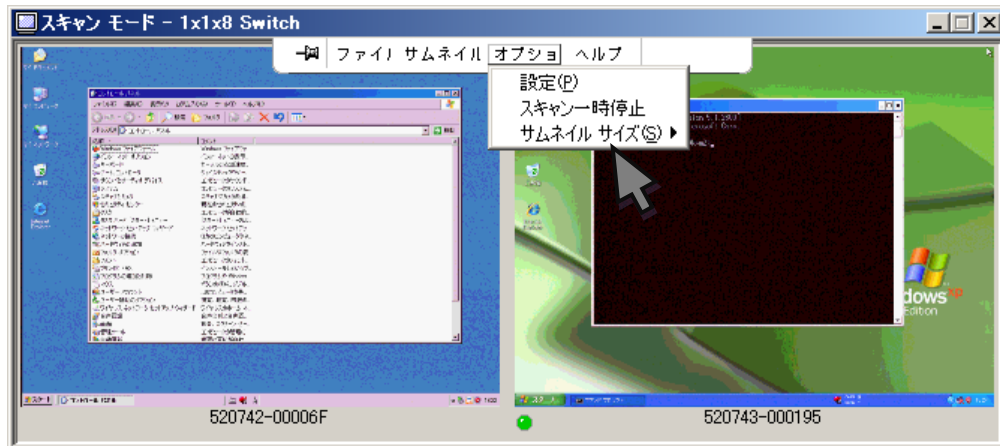
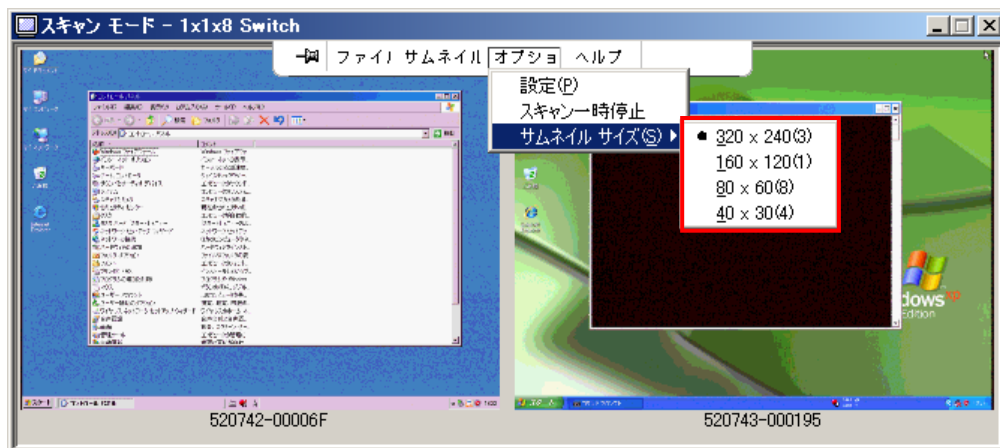
記号	説明
	現在ターゲットデバイスをスキャン中です。
	ターゲットデバイスのスキャンに失敗したことを示します。

フレーム内の画面表示をダブルクリックするとフルサイズ表示となり、マウスおよびキーボード操作も可能となります。

スキャンモードのビデオビューア画面において、マウスカーソルを画面の上端に移動させると下のようなメニューバーが表示されます。このメニューバーから各種設定を行うことができます。

スキャンモードを終了する場合は、メニューバーにおいて、"ファイル"ー"終了" をクリックするか、ウィンドウの右上の「×」ボタンをクリックします。

メニューバーにおいて、"サムネイル"ー"任意のサーバー名"ー"有効化" をクリックすると有効化のチェックの選択／非選択状態が切り替わります。有効化にチェックが入っている状態でスキャンが実行されます。

メニューバーにおいて、”サムネイル”－”任意のサーバー名”－”インターラクティブセッションの表示” をクリックすると、指定したサーバーがフルサイズ表示され、マウスおよびキーボード操作が可能となります。

メニューバーにおいて、"オプション"ー"設定" をクリックすると、下のようなスキャンモード設定ウィンドウが表示されます。

各設定内容は、下のとおりです。

設定内容	説明
デバイス当たりの表示時間	ターゲットデバイス毎のスキャン時間です。 10～60[秒]の範囲で設定します。
デバイスの間の時間	ターゲットデバイスのスキャンを実行してから次のターゲットデバイスのスキャンに移行するまでの時間です。 5～60[秒]の範囲で設定します。

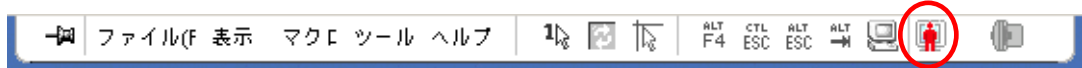
4.14 スキャンモード

メニューバーにおいて、"オプション"ー"スキャン一時停止" をクリックすると、スキャンモードが一時停止します。スキャンモードを再開するには、再度 "オプション"ー"スキャン一時停止" をクリックします。

メニューバーにおいて、"オプション"ー"サムネイルサイズ" をクリックすると、下のように表示され、任意のサムネイルサイズに変更することができます。

任意のサイズを選択するとすぐに設定は適用され、スキャンモードのビューア画面が再表示されます。

モデム経由で接続している場合、スキャンモードは無効です。

4.15. セッションタイプ

ビデオセッションビューアでターゲットデバイスを制御する場合、共有状況に応じて各種のセッションタイプがあります。ビデオセッションビューアのメニューバーに表示されるアイコンから現在のセッションタイプを確認することができます。

ファイル(F 表示 マクロ ツール ヘルプ

セッションタイプの詳細については、下記のとおりです。

セッションタイプ	アイコン表示	内容
アクティブ		KVM セッションの実行中を示します。他のユーザーと制御を共有していない状態です。
ロック		バーチャルメディアセッションとKVMセッションのロックが設定されており、KVM セッションとバーチャルメディアセッションの実行中を示します。
エクスクルーシブ		ターゲットデバイスに対して占有制御権がある状態を示します。 エクスクルーシブモードでの接続中は、他のユーザーとの共有はできません。ただし、管理者によるプリエンプトあるいはステルスモードでのモニターは可能です。
アクティブシェアリング(プライマリ)		他のユーザーとの KVM セッションの共有状態であり、自分が共有を許可したプライマリユーザーであることを示します。
アクティブシェアリング(セカンダリ)		他のユーザーとの KVM セッションの共有状態であり、自分が後で接続を行ったセカンダリユーザーであることを示します。
パッシブシェアリング		ターゲットデバイスのビデオ出力のみを共有し、モニターすることができる状態です。 キーボード、マウス操作はできません。
ステルス		プライマリユーザーの許可なしにターゲットデバイスのビデオ出力をモニターすることができます。プライマリユーザー側には、モニターされていることはわかりません。 ステルスモードのセッションを実行できるのは、管理者ユーザーのみです。

接続の共有について、プライマリユーザー および セカンダリユーザーの定義は、以下のとおりです。

プライマリユーザー : 先にターゲットデバイスにアクセスしているユーザー
セカンダリユーザー : ターゲットデバイスに対して、既にプライマリユーザーが接続している状態で、後でアクセスを実行したユーザー

4.16. プリエンプト操作

ターゲットデバイスへのアクセス権を持つユーザーは、アクセスレベルが同等あるいは下位のユーザーから操作権を強制的に取得することができます。

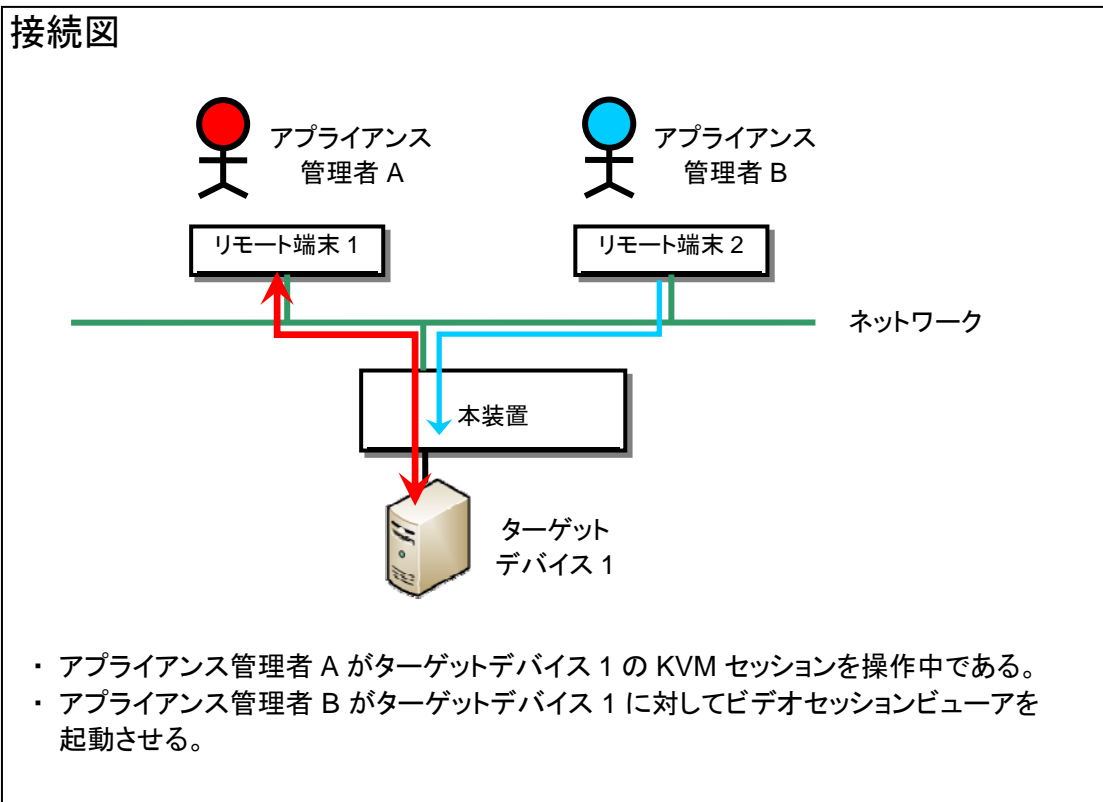
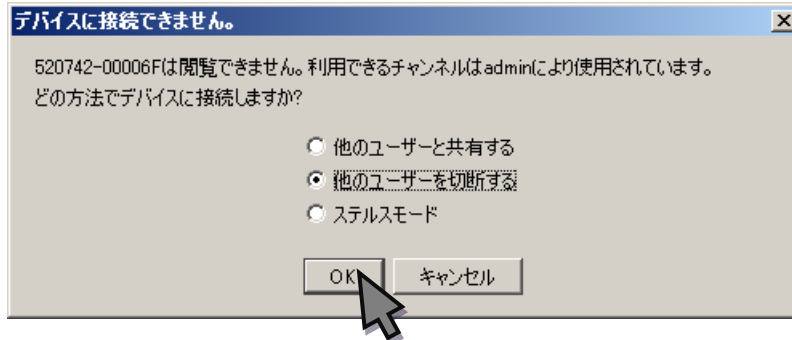
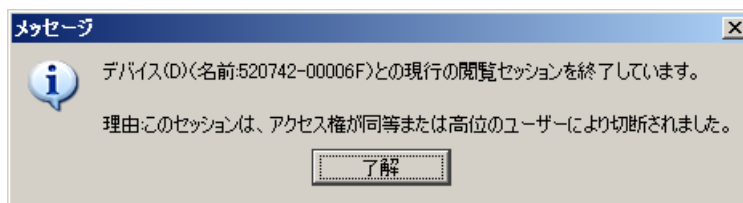
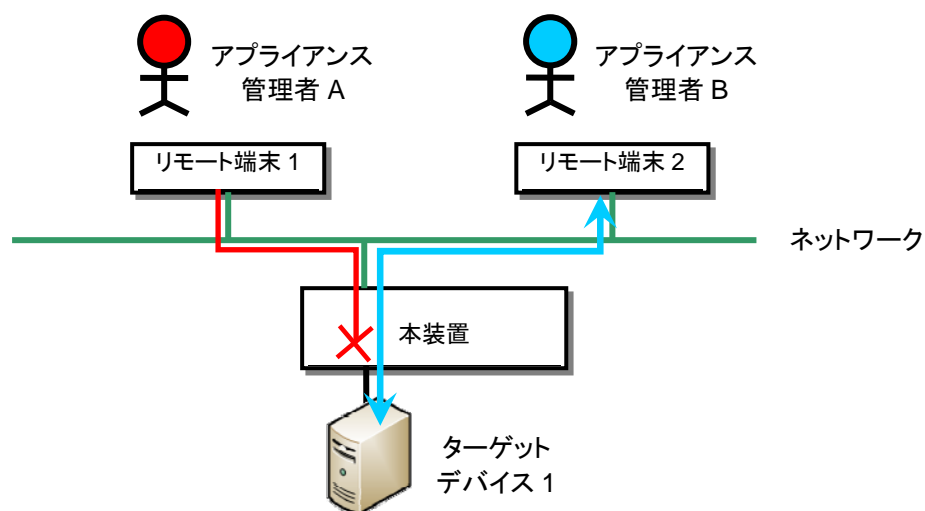
ユーザーアクセスレベルには、OBWI で登録することが可能な アプライアンス管理者、ユーザー管理者、ユーザーの 3 種類があります。また、上記 3 種類とは別に、ローカルの OSD からアクセスするローカルユーザーを含めて、4 種類のアクセス権があります。

アクセスレベルが高い順番は、下記のとおりです。

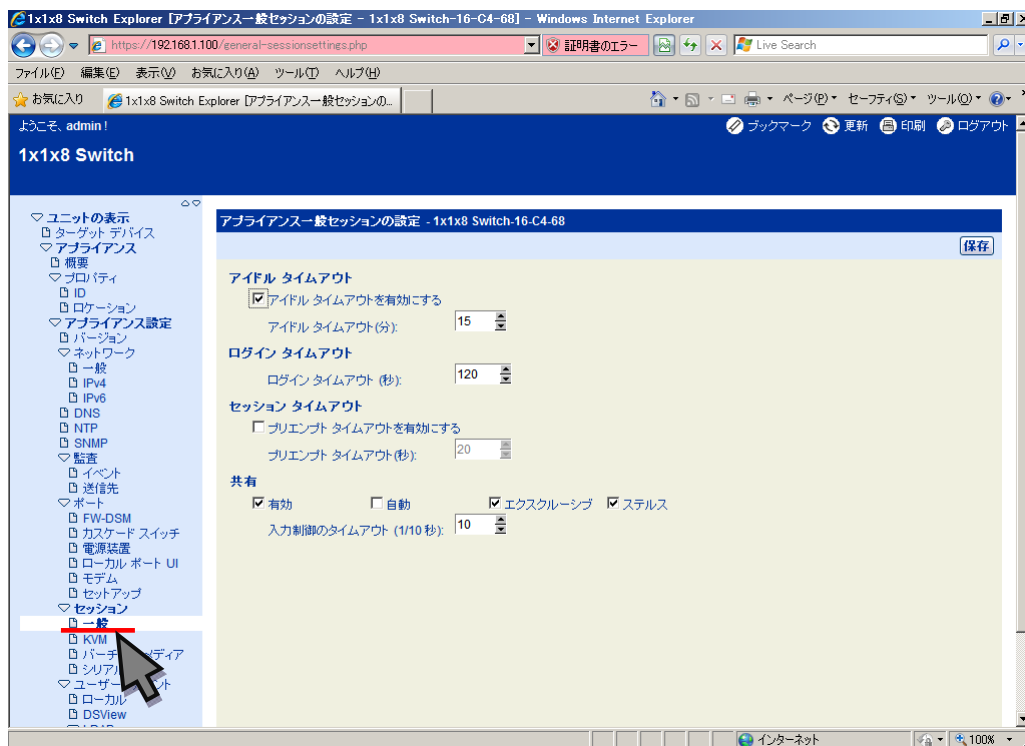
1. アプライアンス管理者、ローカルユーザー（両者のアクセスレベルは同レベル）
2. ユーザー管理者
3. ユーザー

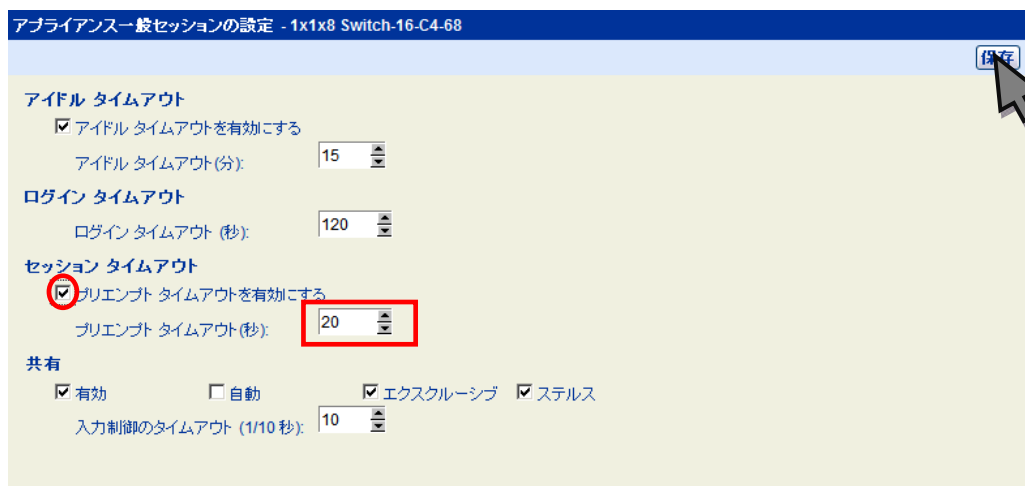
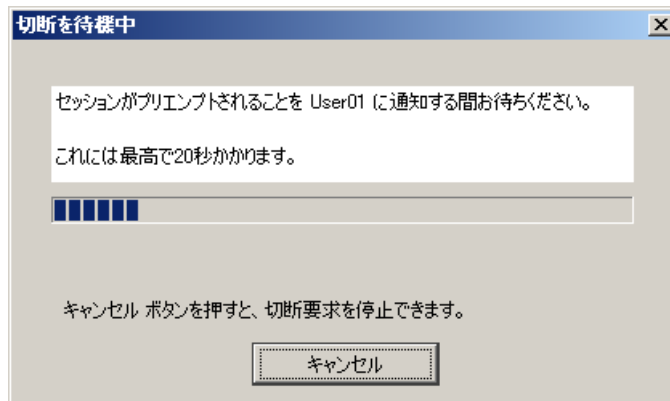
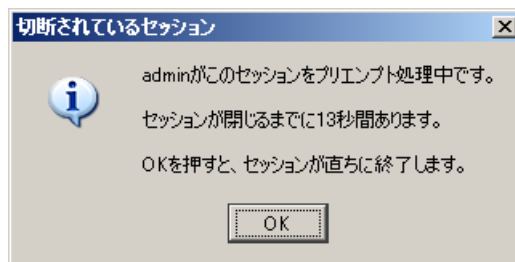
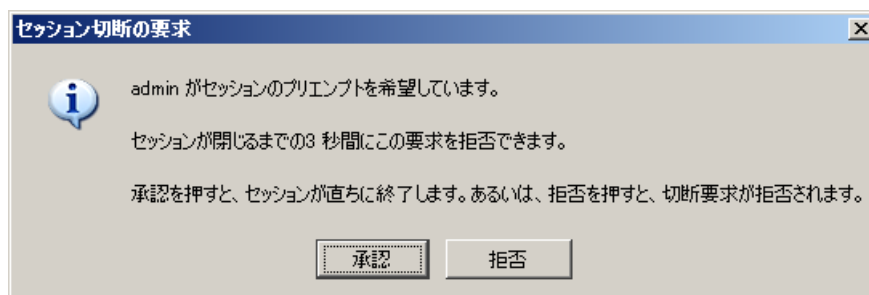
下のような、接続状況を例に説明します。

接続図

- アプライアンス管理者 A がターゲットデバイス 1 の KVM セッションを操作中である。
- アプライアンス管理者 B がターゲットデバイス 1 に対してビデオセッションビューアを起動させる。

アプライアンス管理者 B がターゲットデバイス 1 にアクセスし、ビデオセッションビューアを開こうとするとすると下のようなダイアログが表示されます。
アプライアンス管理者 A から操作権を取得する場合は、"他のユーザーを切断する" を選択し、[OK]ボタンをクリックします。

アプライアンス管理者 A のビデオセッションビューアには、下のようなダイアログが表示され、セッションが強制的に切断されます。

- アプライアンス管理者 B が操作をプリエンプトし、ターゲットデバイス 1 の KVM セッションの操作が可能となる。
- アプライアンス管理者 A の KVM セッションは、強制的に切断される。

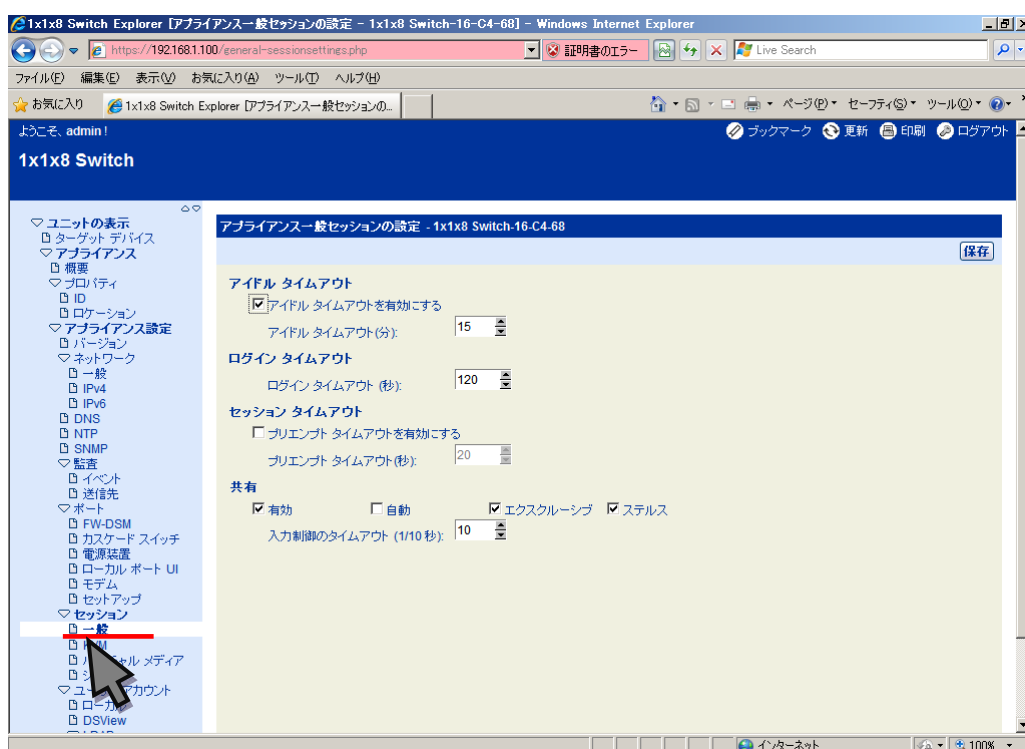
4.16.1 プリエンプトタイムアウトの表示

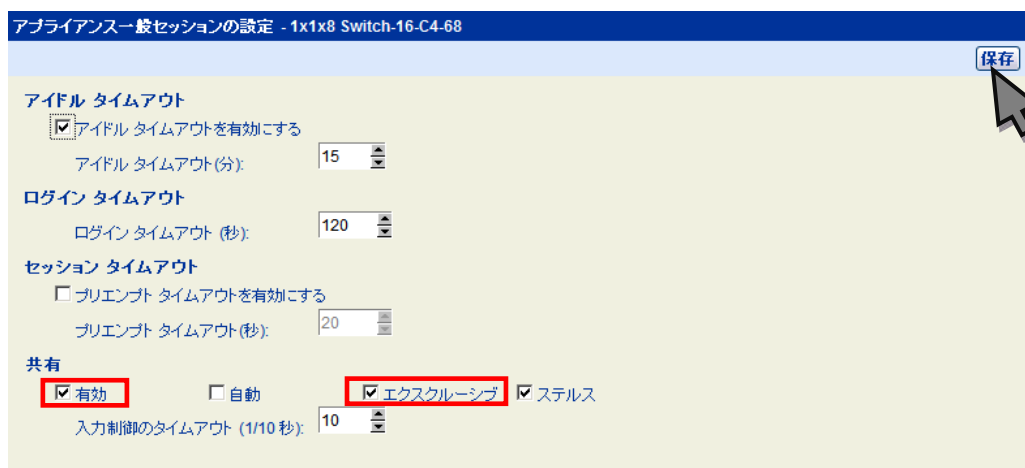
画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「セッション」-「一般」をクリックすると「アプライアンス一般セッションの設定」ページが表示されます。

「プリエンプトタイムアウト」設定において、"プリエンプトタイムアウトを有効にする" にチェックを入れ、「プリエンプトタイムアウト」 に任意の秒数を設定して、右上の[保存]ボタンをクリックするとプリエンプトタイムアウト設定が有効になります。

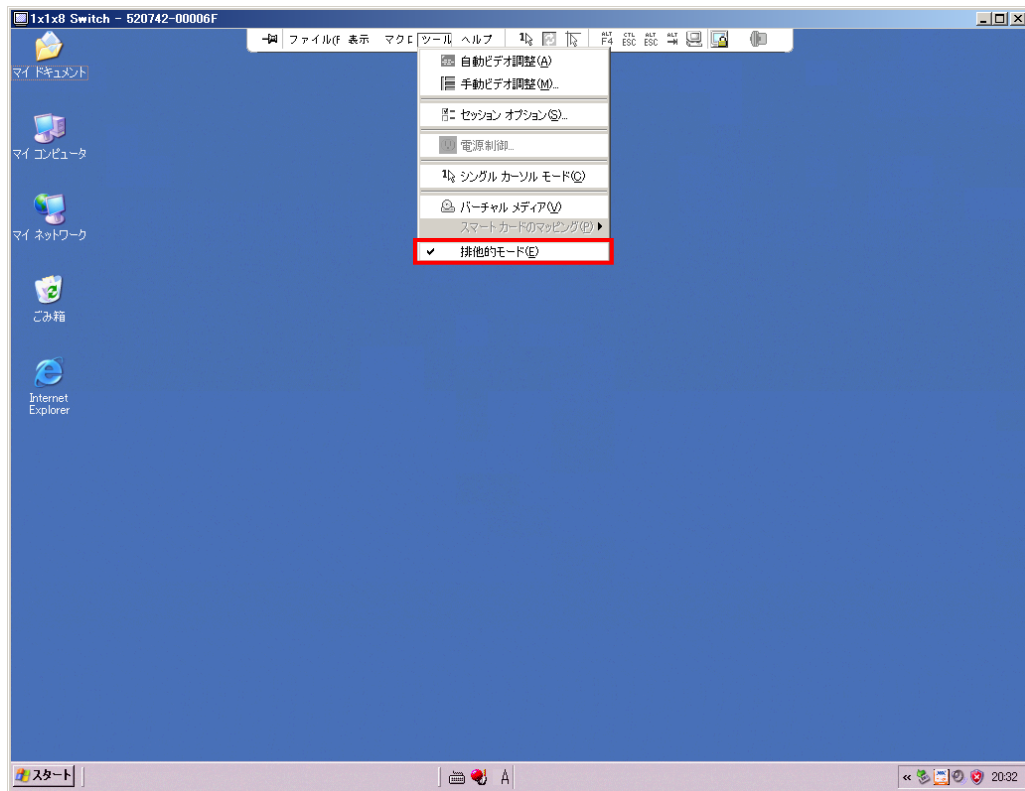
アプライアンス一般セッションの設定 - 1x1x8 Switch-16-C4-68
保存
アイドル タイムアウト
アイドル タイムアウトを有効にする
アイドル タイムアウト(分): 15
ログイン タイムアウト
ログイン タイムアウト (秒): 120
セッション タイムアウト
プリエンプト タイムアウトを有効にする
プリエンプト タイムアウト(秒): 20
共有
有効 自動 エクスクルーシブ ステルス
入力制御のタイムアウト (1/10 秒): 10

プリエンプトする側のユーザーには、下のような "プリエンプションを待機中" メッセージが表示され、「プリエンプトタイムアウト」で設定した秒数のカウントダウンが表示されます。

プリエンプトされる側のユーザーには、下のようにプリエンプトに関する通知メッセージが表示されます。

プリエンプトする側のユーザーとされる側のユーザーのアクセスレベルが同等の場合、プリエンプトされる側のユーザーには、下のような通知メッセージが表示され、プリエンプトを「承認」するか「拒否」するか選択することができます。

4.17. エクスクルーシブモード

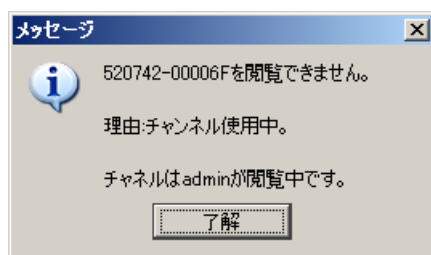
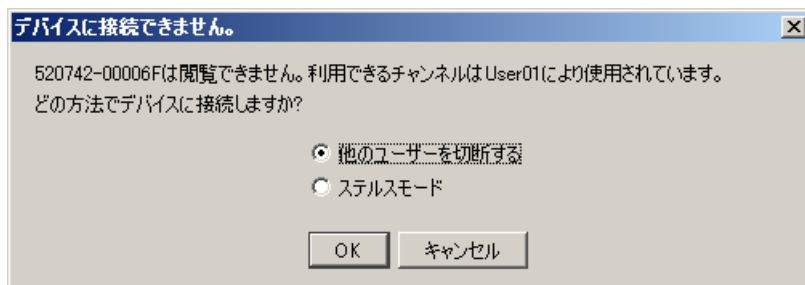
エクスクルーシブモードとは、ビデオセッションビューアを実行している場合、他のユーザーから共有リクエストを受信することなく、独占してターゲットデバイスを操作することができるモードです。

4.17.1 エクスクルーシブモードの有効設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「セッション」-「一般」をクリックすると「アプライアンス一般セッションの設定」ページが表示されます。

「共有」項目の ”有効” および ”エクスクルーシブ” にチェックをいれ、[保存]ボタンをクリックします。

アプライアンス一般セッションの設定 - 1x1x8 Switch-16-C4-68
保存
アイドル タイムアウト
アイドル タイムアウトを有効にする
アイドル タイムアウト(分): 15
ログイン タイムアウト
ログイン タイムアウト (秒): 120
セッション タイムアウト
プリエンプト タイムアウトを有効にする
プリエンプト タイムアウト(秒): 20
共有
有効 自動 エクスクルーシブ ステルス
入力制御のタイムアウト (1/10 秒): 10

4.17.2 エクスクルーシブモードの実行

下のように、ビデオセッションビューアの メニューバーにおいて、"ツール"ー"排他的モード" をクリックすると、エクスクルーシブモードが有効になり、("排他的モード" 表示の左側にチェックが入ります。)他のユーザーからの共有リクエストは拒否されます。

エクスクルーシブモードが有効になるとビデオセッションビューアのメニューバーにおいて、下のようなアイコン表示となります。

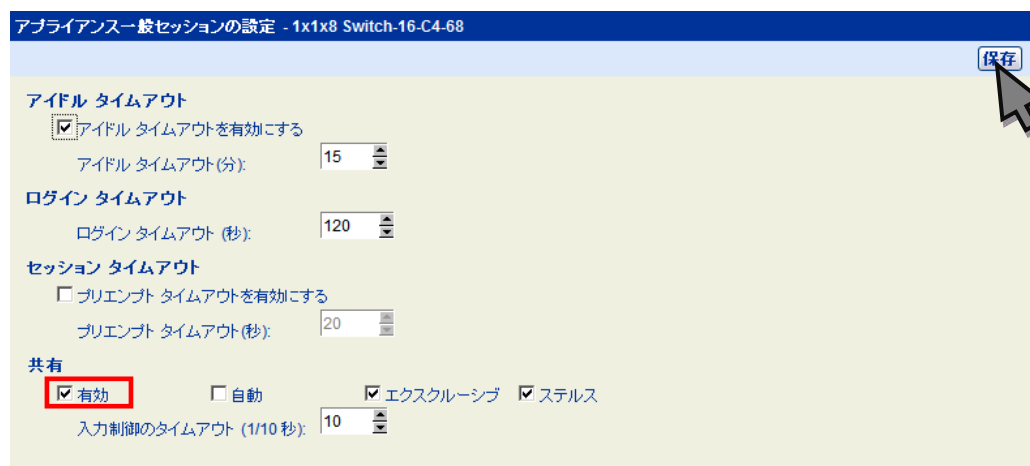
アプライアンス管理者 A がターゲットデバイス 1 の KVM セッションをエクスクルーシブモードで接続中の状態において、2 番目にアクセスしたユーザーには、下のように表示され、アクセスは拒否されます。

ただし、アプライアンス管理者がセカンダリユーザーとしてアクセスした場合は、下のようなダイアログが表示され、プリエンプトするかステルスモードでモニターするかを選択することができます。

参照 4.19 ステルスモード（210 ページ）

4.18. 共有モード

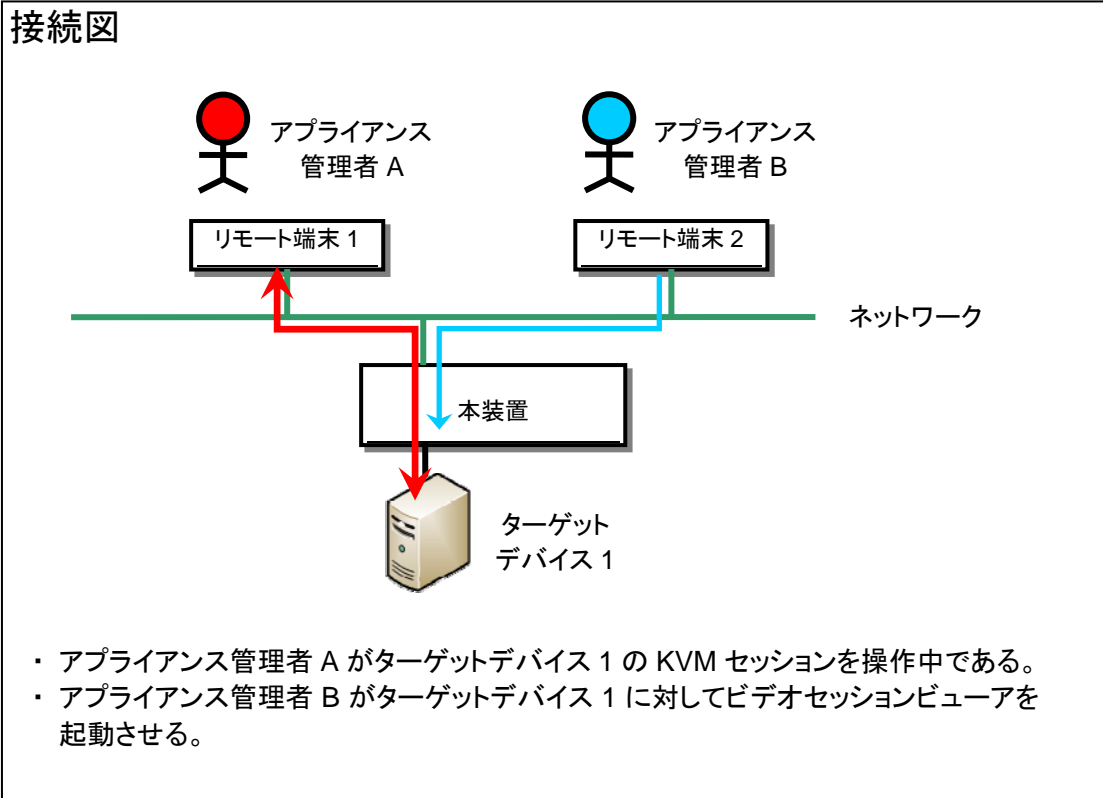
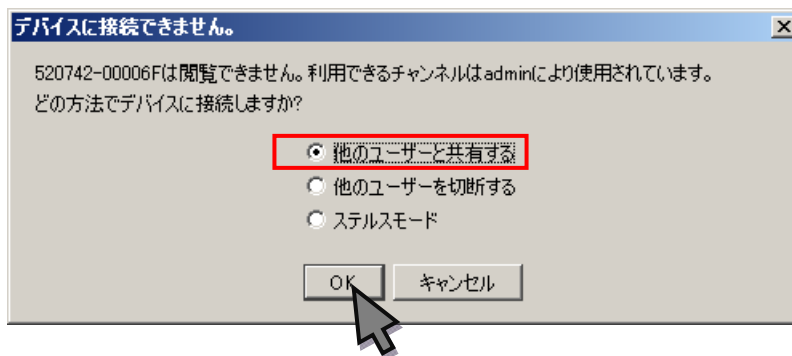
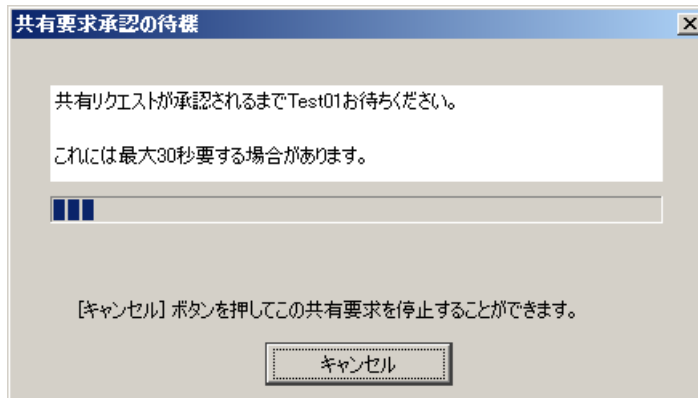
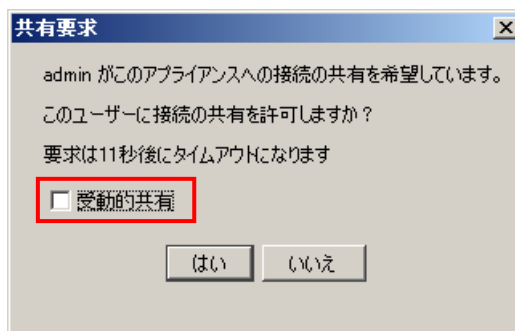
共有してターゲットデバイスを操作するモードには、2 種類があります。一つは、複数のユーザーがターゲットデバイスの操作を交代で行うことができるアクティブシェアリング。もう一つは、プライマリユーザーのみがターゲットデバイスの制御権を持ち、他のユーザーは、ビデオデータの表示(モニター)のみが許可されるパッシブシェアリングです。

4.18.1 共有モードの有効設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「セッション」-「一般」をクリックすると「アプライアンス一般セッションの設定」ページが表示されます。

「共有」項目の "有効" にチェックをいれ、[保存]ボタンをクリックします。

4.18.2 共有モードの実行

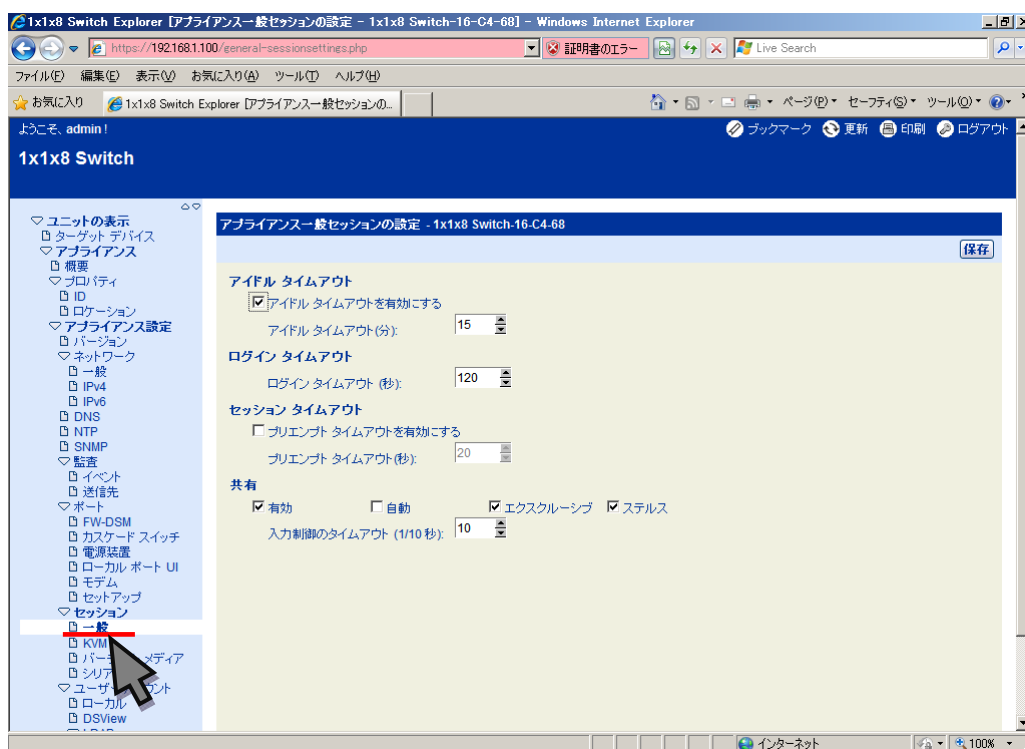
下のような、接続状況を例に説明します。

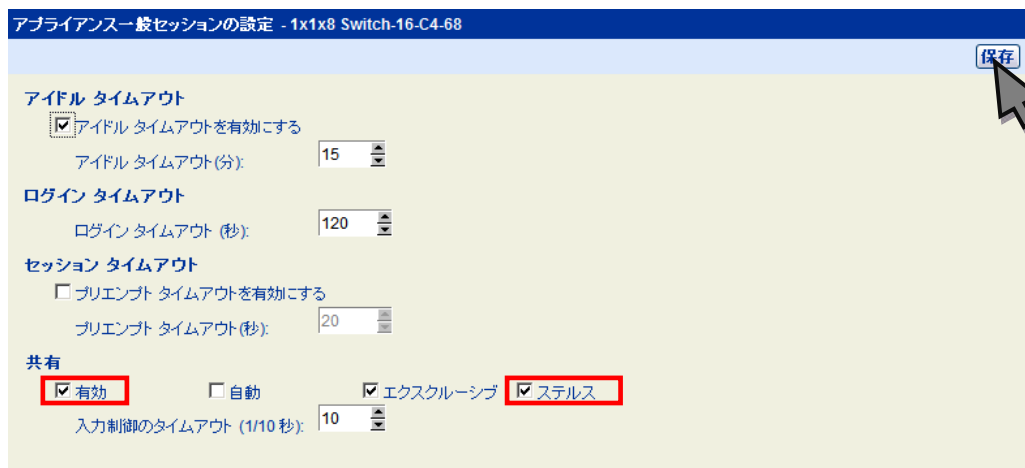
・ アプライアンス管理者 A がターゲットデバイス 1 の KVM セッションを操作中である。
・ アプライアンス管理者 B がターゲットデバイス 1 に対してビデオセッションビューアを起動させる。

アプライアンス管理者 B がターゲットデバイス 1 にアクセスし、ビデオセッションビューアを起動させようとすると下のようなダイアログが表示されます。
共有モードでビデオセッションビューアを起動する場合は、"他のユーザーと共有する" を選択し、[OK]ボタンをクリックします。

下のように、"共有リクエスト承認の待機" ダイアログが表示されます。ここでプライマリユーザー(アプライアンス管理者 A)に共有モードが承認されるのを待ちます。

プライマリユーザー(アプライアンス管理者 A)には、下のようなダイアログが表示されます。

アクティブシェアリングを許可する場合は、そのまま[はい]ボタンをクリックします。
パッシブシェアリングを許可する場合は、"受動的共有" チェックボックスにチェックを入れ、[はい]ボタンをクリックします。
共有モードを拒否する場合は、[いいえ]ボタンをクリックします。

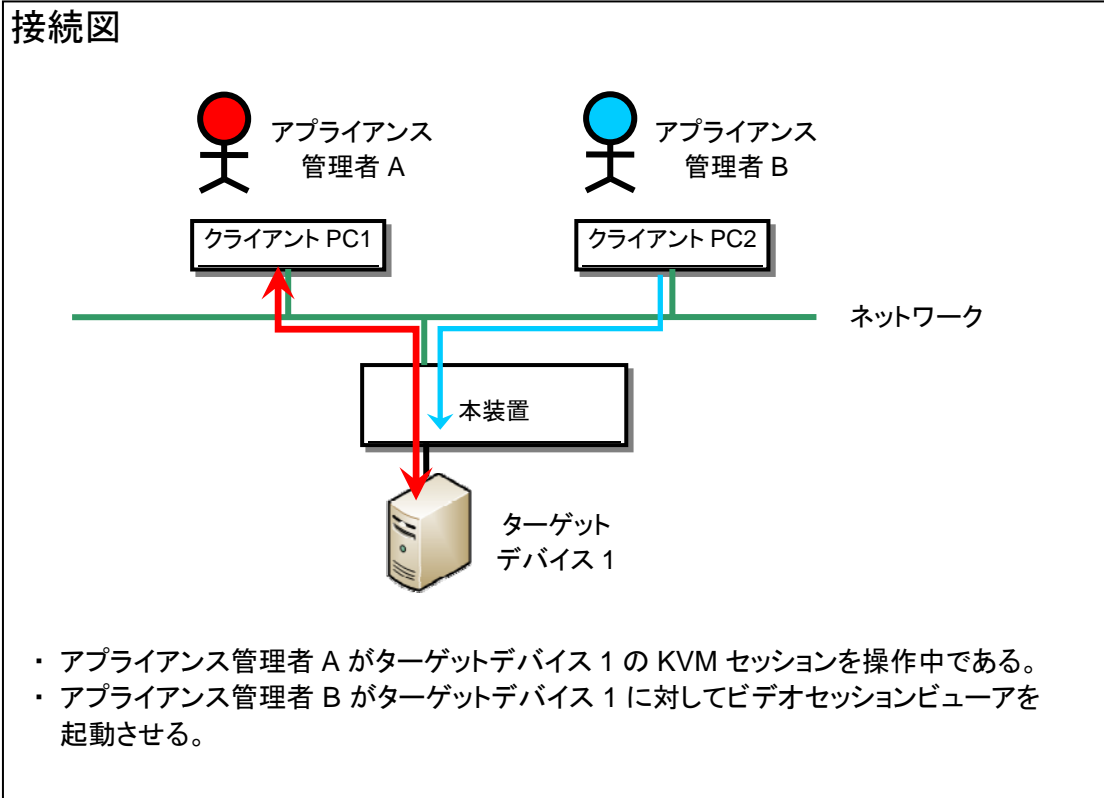
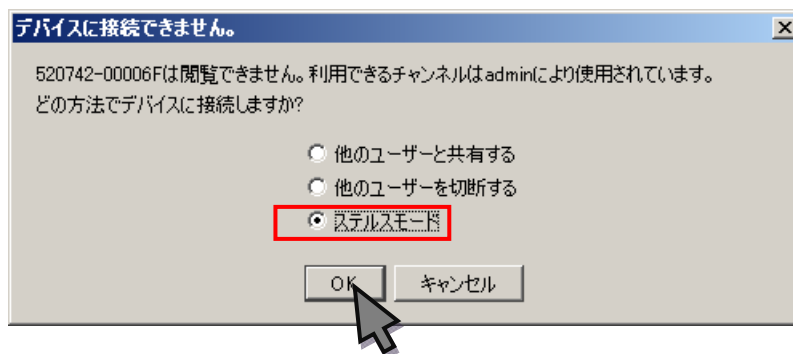
4.19. ステルスモード

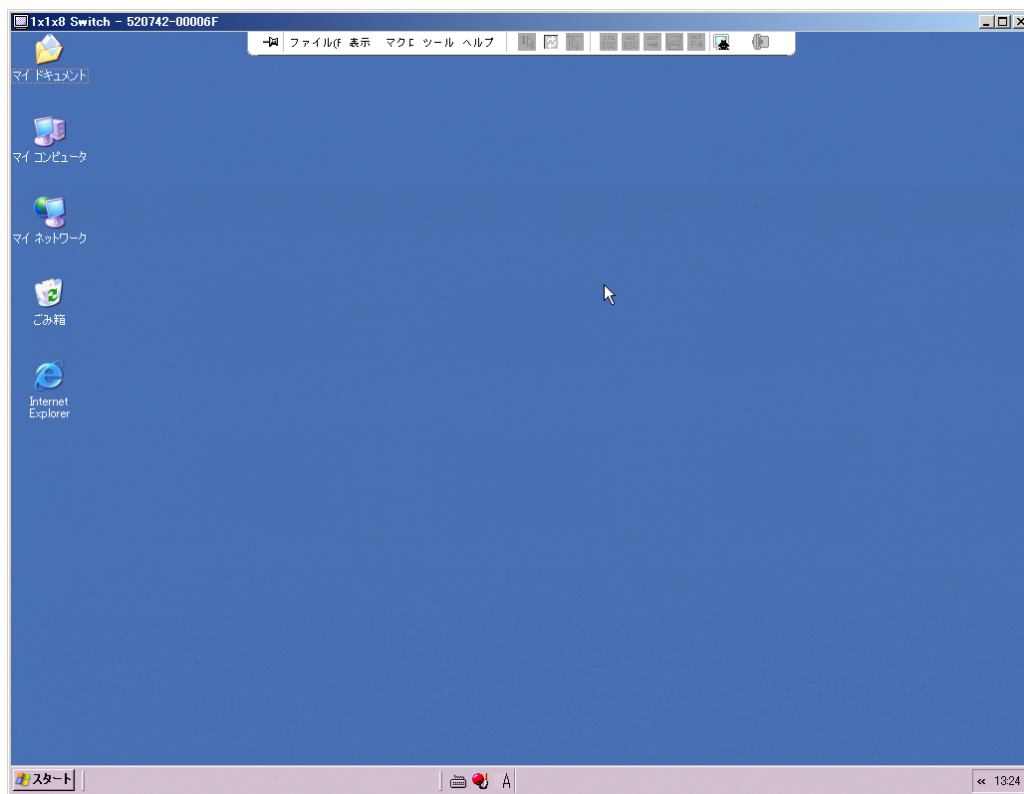
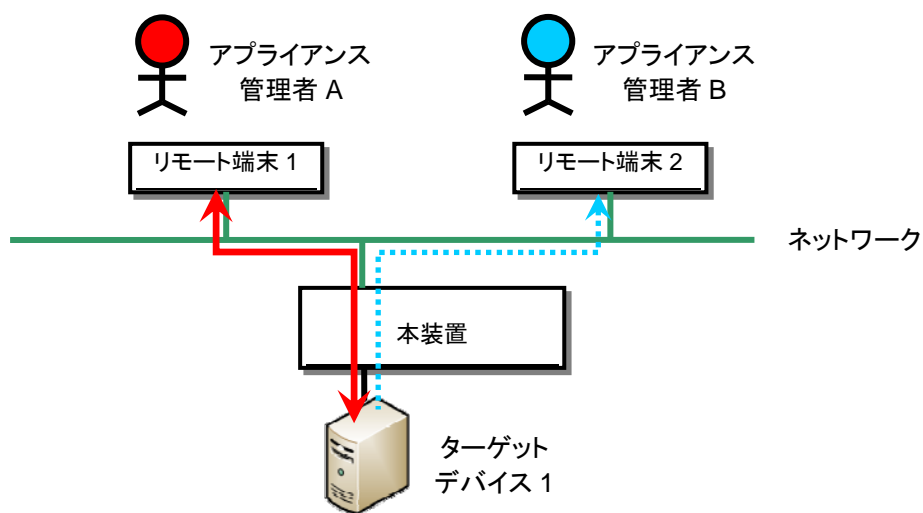
ステルスモードとは、アプライアンス管理者が他のユーザーによって接続されているターゲットデバイスに対し、接続中のプライマリユーザーにはわからない状態でビデオデータのみをモニターする接続モードです。

4.19.1 ステルスモードの有効設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「セッション」-「一般」をクリックすると「アプライアンス一般セッションの設定」ページが表示されます。

「共有」項目の ”有効” および ”ステルス” にチェックを入れ、[保存]ボタンをクリックします。

アプライアンス一般セッションの設定 - 1x1x8 Switch-16-C4-68
保存
アイドル タイムアウト
アイドル タイムアウトを有効にする
アイドル タイムアウト(分): 15
ログイン タイムアウト
ログイン タイムアウト (秒): 120
セッション タイムアウト
プリエンプト タイムアウトを有効にする
プリエンプト タイムアウト(秒): 20
共有
有効　自動　エクスクルーシブ　ステルス
入力制御のタイムアウト (1/10 秒): 10

4.19.2 ステルスモードの実行

下のような、接続状況を例に説明します。

アプライアンス管理者 B がターゲットデバイス 1 にアクセスし、ビデオセッションビューアを開こうとするとすると下のようなダイアログが表示されます。
ステルスモードでビデオセッションビューアを起動する場合は、"ステルスモード" を選択し、[OK]ボタンをクリックします。

ステルスモードでビデオセッションビューアが起動し、メニューバーのアイコンが下のような表示となります。

メニューバー上の設定に関するボタンは、全てグレイアウト状態となり、マウスおよびキーボード操作を行うことはできません。

- アプライアンス管理者 B がステルスモードで接続。ビデオのモニタリングのみ可能。
- アプライアンス管理者 A のターゲットデバイス 1 の KVM セッションは継続する。アプライアンス管理者 A は、アプライアンス管理者 B がステルスモードで接続していることはわからない。

4.20. シリアルデバイスの操作

サーバーユニット FW-DSM03/SRL を使用して、RS232C シリアルデバイスを制御する操作方法について説明します。
FW-DSM03/SRL は、添付の USB 電源ケーブルを用いて、ターゲットデバイスの USB ポートから電源供給を受けるか、オプション（別売）の電源アダプタを使用して電源を供給する必要があります。

FW-DSM03/SRL をご購入いただきますと以下の物品が含まれています。

サーバーユニット本体

変換アダプタ（D-sub9 メス⇔RJ45）

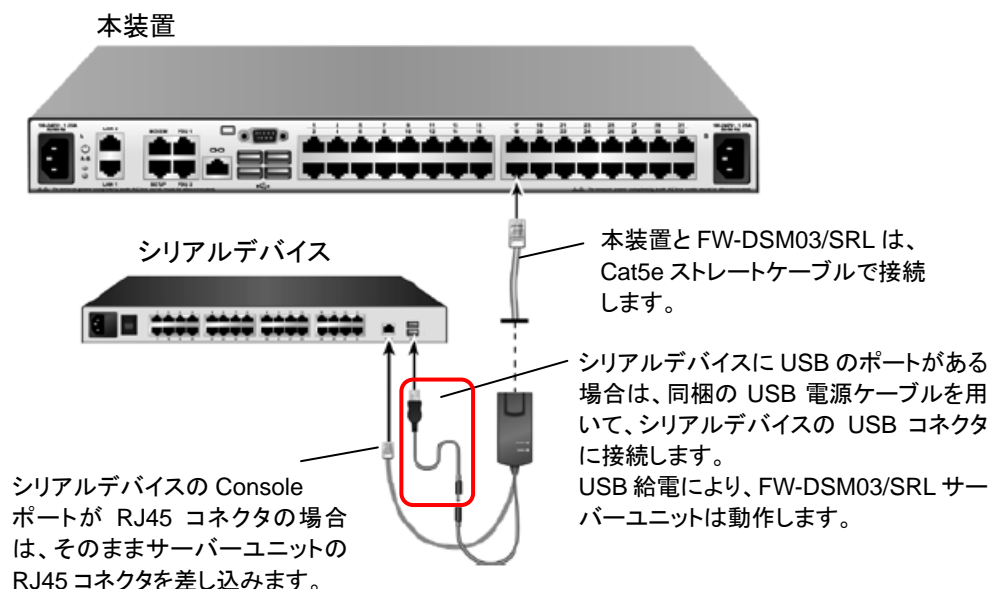
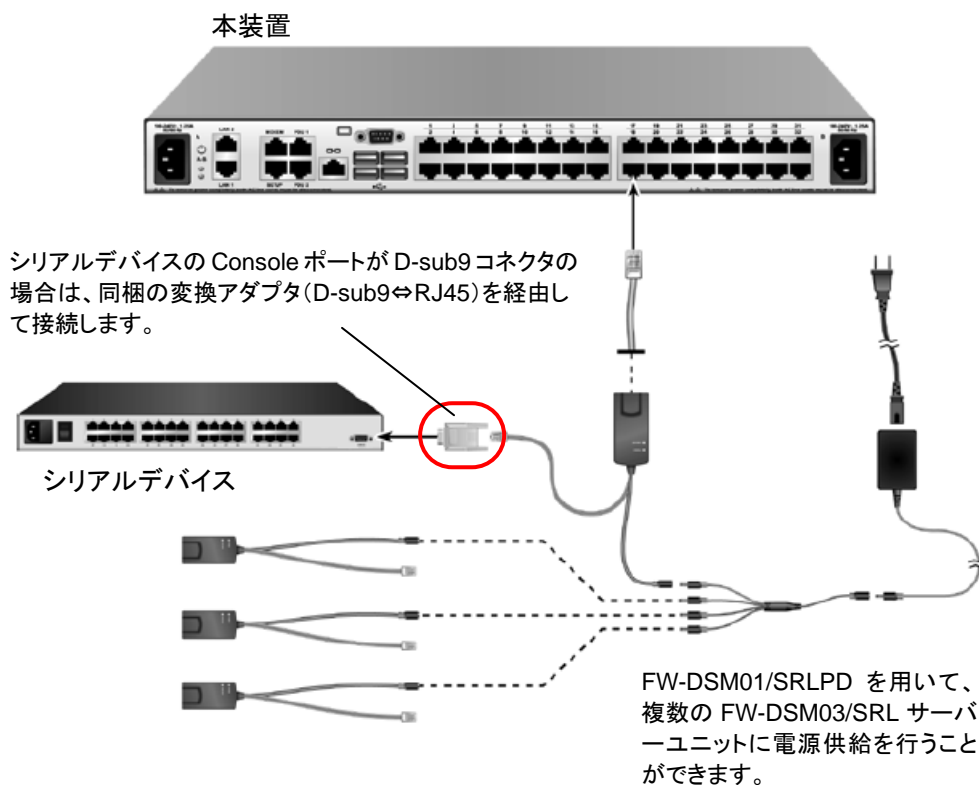
USB 電源ケーブル

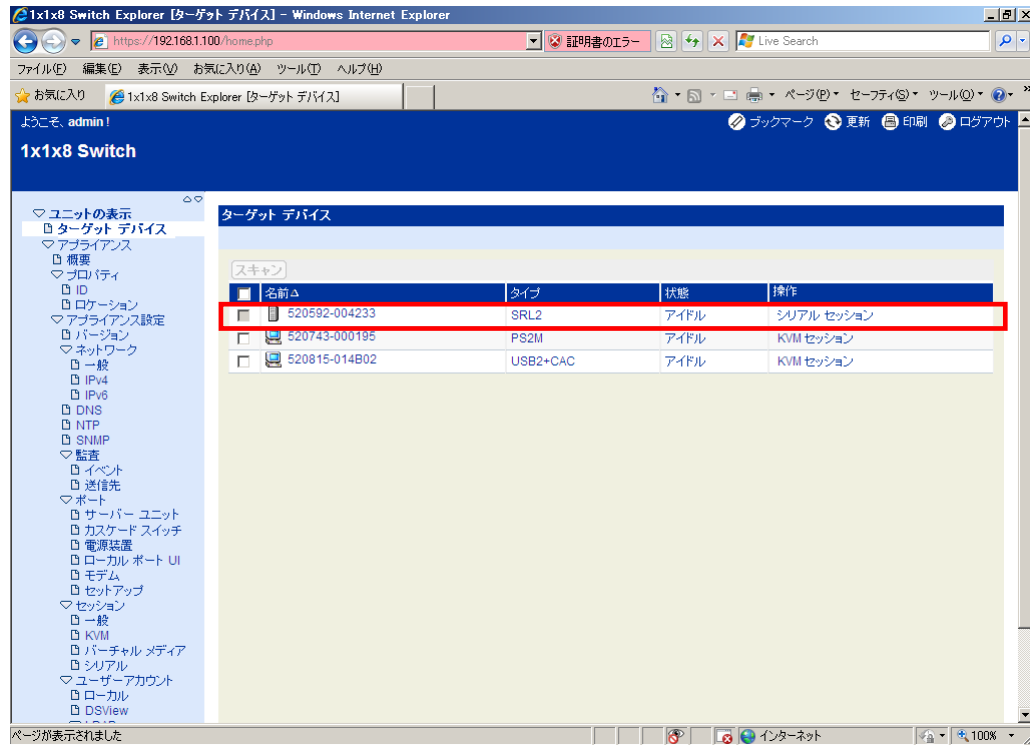
また、上記サーバーユニット FW-DSM03/SRL 用の電源アダプタ FW-DSM01/SRLPD もオプションとしてご購入いただくことができます。下の物品を含んでいます。

電源アダプタ

電源拡張用ケーブル

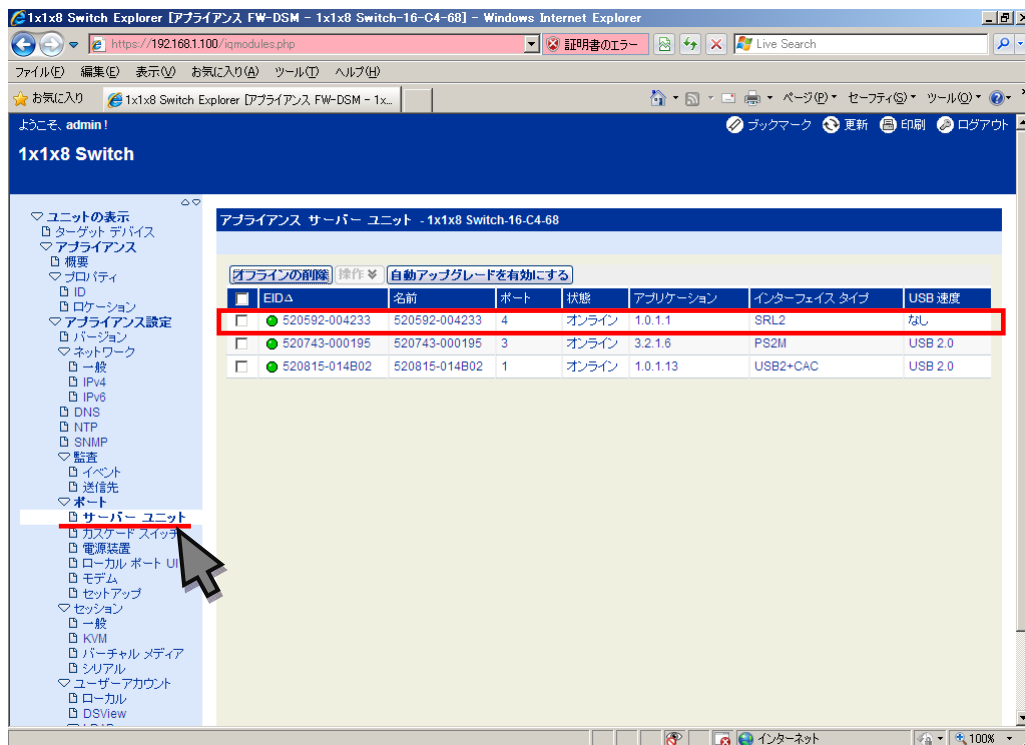
4.20.1 シリアルデバイスの接続構成

本装置にサーバーユニット FW-DSM03/SRL を用いてシリアルデバイスを接続する構成を以下に示します。

また、電源アダプタ FW-DSM01/SRLPD を用いて、FW-DSM03/SRL に電源供給する場合の接続構成を示します。

4.20.2 シリアルデバイスの画面表示

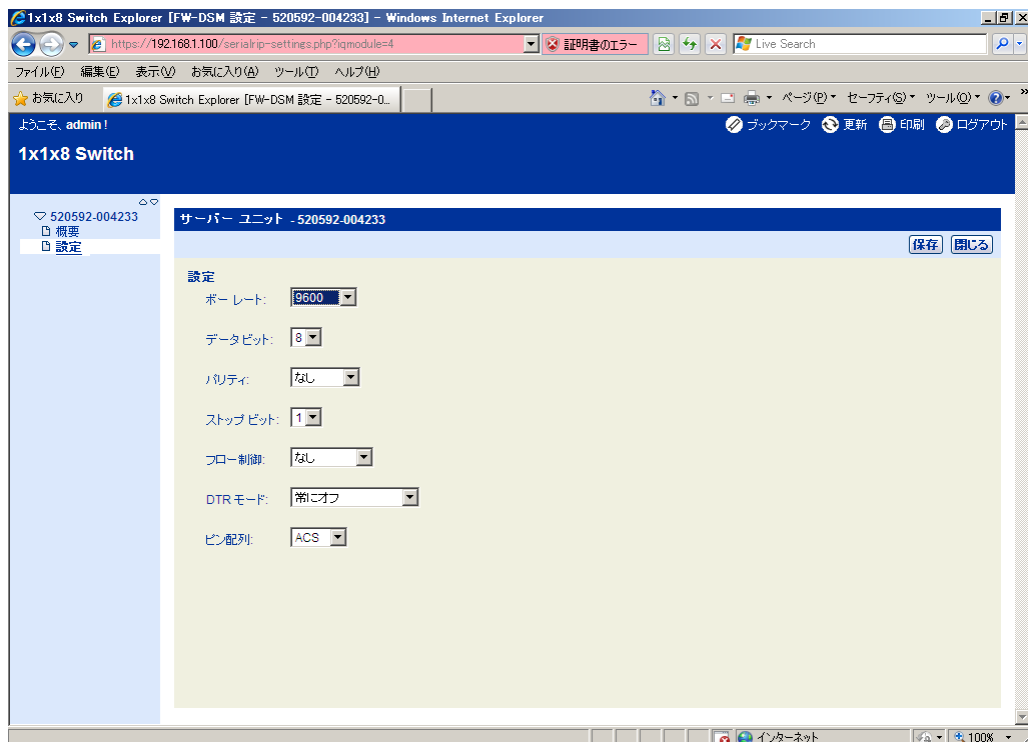
サーバーユニット FW-DSM03/SRL を用いてシリアルデバイスを接続し、本装置に認識されると OBWI の「ターゲットデバイス」ページの一覧に下のように表示されます。

サーバーユニット FW-DSM03/SRL については、 アイコン表示されます。

4.20.3 シリアル通信の設定

画面左のメニュー選択領域において、「ユニットの表示」-「アプライアンス」-「アプライアンス設定」-「ポート」-「サーバーユニット」をクリックすると「アプライアンス サーバーユニット」ページが表示されます。ターゲットのシリアルデバイスがサーバーユニット FW-DSM03/SRL を用いて本装置に接続されている場合、下のようにリスト表示されます。

サーバーユニット FW-DSM03/SRL の場合、「インターフェースタイプ」項目に ”SRL2” と表示されます。

サーバーユニット FW-DSM03/SRL の EID をクリックします。

下のように、サーバーユニット F03/SRL の情報が表示されます。ここで、画面左のメニュー選択領域において、「設定」をクリックします。

下のような「サーバーユニットの設定」画面が表示されます。

ここでシリアル通信の設定を行います。

各設定の内容は、下記のとおりです。

項	設定項目	内容
1	ボーレート	シリアルポート通信の速度を設定します。 以下から選択します（単位: bps）。 50, 75, 110, 150, 200, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200
2	データビット	シリアルポート通信のデータビット数を設定します。 以下から選択します。 7, 8
3	パリティ	シリアルポート通信のパリティを設定します。 以下から選択します。 なし、偶数、奇数、マーク、スペース
4	ストップビット	シリアルポート通信のストップビット数を設定します。 以下から選択します。 1, 2
5	フロー制御	シリアルポート通信のフロー制御タイプを設定します。 以下から選択します。 なし ：フロー制御を無効にします。 XON/XOFF ：X フロー制御を有効にします。 RTS/CTS ：RTS/CTS フロー制御を有効にします。
6	DTR モード	DTR 線をどのように制御するか設定します。 常にオフ ：DTR 線は常にオフ状態となります。 接続時に有効にする ：DTR 線はシリアル接続時に有効となります。
7	ピン配列	シリアルポートのピン配列を設定します。 以下から選択します。 ACS ：次のページの「ACS ポート ピン配列」をご参照ください。 Cisco ：次のページの「Cisco ポート ピン配列」をご参照ください。

「ピン配列」設定の詳細

”ACS” ポート ピン配列

ピン番号	信号名	IN/OUT
1	RTS (Request to Send)	OUT
2	DTR (Data Terminal Ready)	OUT
3	TxD (Transmit Data)	OUT
4	GND (Signal Ground)	---
5	CTS (Clear to Send)	IN
6	RxD (Receive Data)	IN
7	DCD/DSR (Data Set Ready)	IN
8	N/C (Not Connected)	---

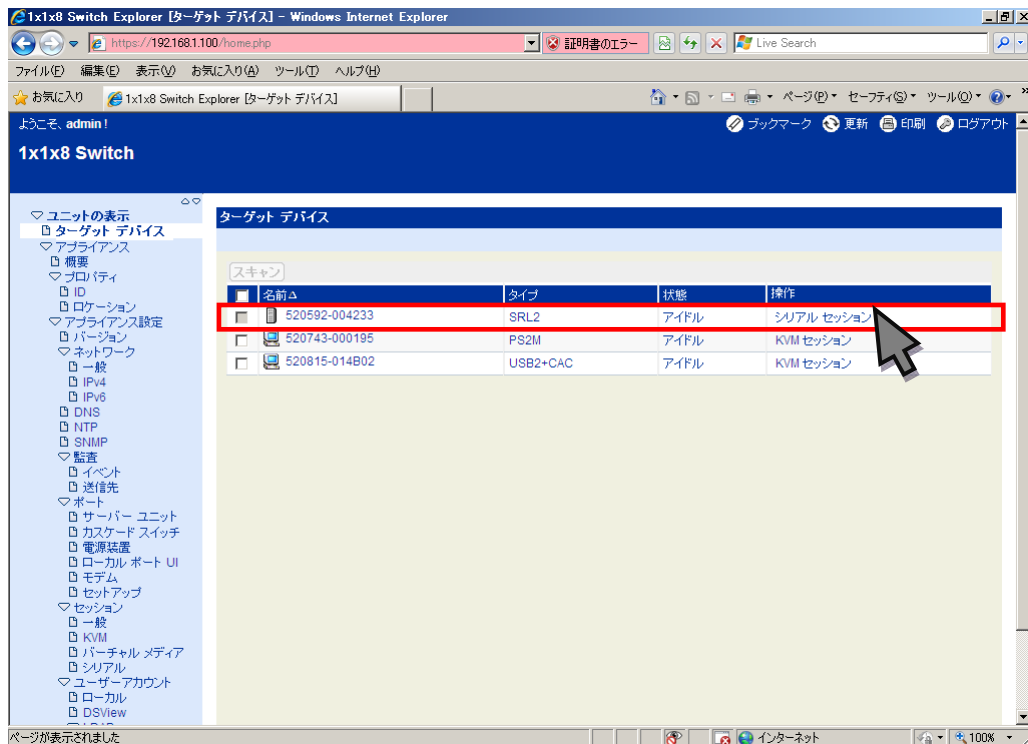
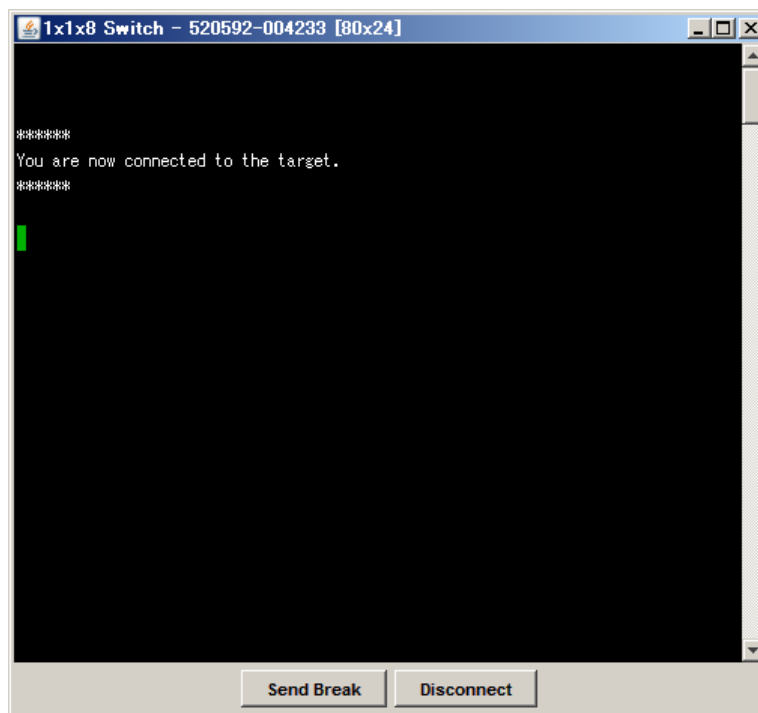
ターゲットのシリアルデバイスとの接続において、D-sub9⇔RJ45 変換アダプタを使用している場合は、ピン配列の設定を ”ACS” にします。

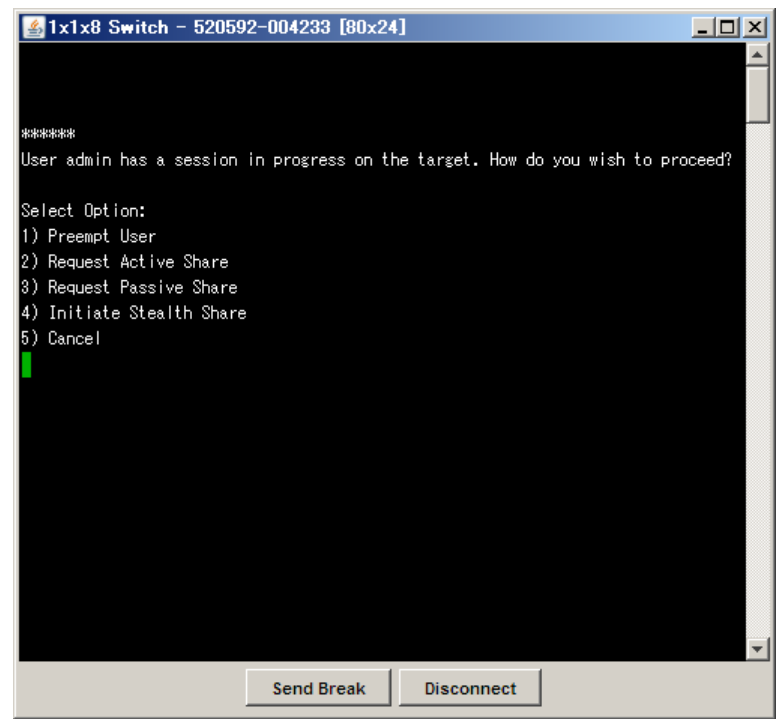
”Cisco” ポート ピン配列

ピン番号	信号名	IN/OUT
1	CTS (Clear to Send)	IN
2	DCD/DSR (Data Set Ready)	IN
3	RxD (Receive Data)	IN
4	GND (Signal Ground)	---
5	N/C (Not Connected)	---
6	TxD (Transmit Data)	OUT
7	DTR (Data Terminal Ready)	OUT
8	RTS (Request to Send)	OUT

ターゲットデバイスとなるシリアルデバイスが Cisco 製品あるいは、Cisco 製品と同様のピン配列の機器の場合は、ピン配列の設定を ”Cisco” にします。

4.20.4 シリアルビューアの起動

OBWI から サーバーユニット FW-DSM03/SRL が接続されたシリアルデバイスを操作するためには、下のようにターゲットデバイスリストの "シリアルセッション" をクリックします。

シリアルビューア画面が表示され、ターゲットデバイスの操作が可能となります。

4.20.5 シリアルビューアの共有設定

ターゲットのシリアルデバイスに対して、既に別のユーザーがアクセスしている状態において、自分がアクセスした場合、シリアルビューア画面に下のように表示されます。

共有のオプションとして下記の 4 種類から選択することができます。

項	設定項目	内容
1	Preempt User	1 を入力するとプリエンプト操作を実行します。 ターゲットデバイスへのアクセス権を持つユーザーは、アクセスレベルが同等あるいは下位のユーザーから操作権を強制的に取得することができます。 📖 参照 4.16 プリエンプト操作（200 ページ）
2	Request Active Share	2 を入力するとアクティブシェアリングでの共有接続を要求します。アクティブシェアリングでは、複数のユーザーがターゲットデバイスの操作を交代で行うことができます。 📖 参照 4.18 共有モード（207 ページ）
3	Request Passive Share	3 を入力するとパッシブシェアリングでの共有接続を要求します。パッシブシェアリングでは、プライマリユーザーのみがターゲットデバイスの制御権を持ち、他のユーザーは、ビデオデータの表示（モニター）のみが許可されます。 📖 参照 4.18 共有モード（207 ページ）
4	Initiate Stealth Share	4 を入力するとステルスモードでの接続を開始します。 ステルスモードとは、優先ユーザーに認識されることなく、ビデオ表示のみを共有する接続モードです。 📖 参照 4.19 ステルスモード（210 ページ）

1～4 の項目を入力すると任意の共有モードでの動作が実行されます。
ビューア画面の下の[Send Break]ボタンをクリックすると、ターゲットデバイスに Break 信号が送信されます。また、[Disconnect]ボタンをクリックするとセッションが終了し、ビューア画面は閉じます。

4.20.6 Telnet によるシリアルアクセス

OBWI の「シリアルセッションの設定」において、Telnet アクセスが有効になっている場合、OBWI を介さずに直接 Telnet アクセスによって、シリアルデバイスにアクセスすることができます。

参照 3.27 シリアルセッションの設定 （133 ページ）

以下に Telnet アクセスの手順について説明します。

本装置の IP アドレスに対して Telnet アクセスすると、下のように "Username" プロンプトが表示されます。ターゲットのシリアルデバイスへのアクセス権限を持つユーザー名を入力します。

```
Username: admin Enter↵
```

"Target Name" プロンプトが表示されます。サーバーユニット FW-DSM03/SRL に設定されている名称を入力します。設定名称は、OBWI の「ターゲットデバイス」ページのリスト一覧から確認することができます。

```
Username: admin
Target Name: 520592-004233 Enter↵
```

"Password" プロンプトが表示されます。ユーザーパスワードを入力します（パスワードは表示されません）。

```
Username: admin
Target Name: 520592-004233
Password: 〈表示されません〉 Enter↵
```

パスワード認証およびターゲット名称に問題がなければ、下のように表示され、シリアルデバイスの操作が可能となります。

```
Username: admin
Target Name: 520592-004233
Password:


******
You are now connected to the target.
******
```

Chapter 5 -　　シリアルコンソール

本装置をシリアルコンソールから操作する方法について説明しています。

5

シリアルコンソール

本章の内容

5.1. シリアルコンソール操作の概要

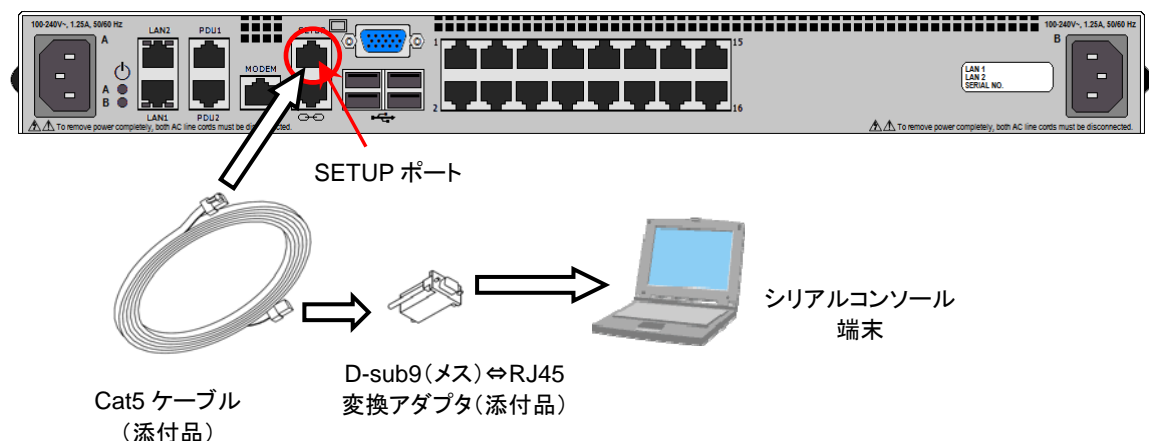
本装置背面の SETUP ポートに添付の専用ケーブルおよび変換アダプタを用いて、シリアルコンソール端末と接続することにより、シリアルコンソール操作が可能となります。

シリアルコンソールから実行可能な設定あるいは操作内容は、下記のとおりです。
1. ネットワーク設定（速度設定、IP アドレス設定、SSLv2 設定）
2. 装置デバッグメッセージの出力
3. 装置の再起動

主に、設置の際の初期設定などのためにシリアルコンソールからの操作インターフェースを用意しています。その他の設定については、OBWI やローカルポート UI の設定画面から行うことができます。

5.2. シリアルコンソール端末の接続方法

シリアルコンソール端末の接続方法について、下記に示します。

［FW-D2116NP の場合］

重要

本製品のシリアルコンソールのピン配置は独自配置により、一般的な Cisco 互換のピン配置ではありません。このシリアルコンソールを D-Sub9 を介した 232c インターフェースに変換するには、上記の Cat ケーブル(銀色の平たいケーブル)と D-Sub9(メス)⇔RJ45 変換アダプタが必須です。

5.3. シリアルコンソールへの接続

本装置のシリアルコンソールポートから実行できる操作について説明します。

① 本装置の SETUP ポートとシリアルコンソール端末を接続します。
📖 参照 5.2 シリアルコンソール端末の接続方法（224 ページ）

② シリアルコンソール端末上のエミュレータ・アプリケーション（ハイパーターミナルなど）を起動し、以下のようにパラメーターを設定します。

通信条件	設定値
ボーレート	9600bps
データ長	8bit
パリティ	なし
ストップビット	1bit

③ 本装置が起動している状態で、Enter キーを入力すると、下のような Main Menu 画面が表示されます。ここで各種設定が可能です。

```
+--------------------------------------------------+
|              2x1x16 Switch Console               |
|                                                  |
|                   1.18.0.22011                   |
|                                                  |
|  Copyright (c) 2000-2012, All Rights Reserved   |
+--------------------------------------------------+
|                IP Configuration                  |
+--------------------------------------------------+

      1. Network Configuration
      2. Enable Debug Messages
      3. Reset Appliance
      0. Exit

  Enter selection ->
```

Main Menu コマンド内容

番号	設定内容	📖 参照
1	ネットワーク速度、IP アドレス設定、SSL 設定などネットワークに関する設定を行います。	226 ページ
2	デバッグメッセージ出力の有効／無効を設定します。	236 ページ
3	本装置を再起動します。	237 ページ
0	ログアウトします。	

5 シリアルコンソール

5.4.　ネットワーク設定

ネットワーク設定メニューでは、下記のような設定を行うことができます。

① ネットワーク速度
② IP の設定（DHCP/固定、IPv4/IPv6）
③ IP アドレス
④ ネットマスク
⑤ デフォルトゲートウェイ
⑥ OBWI における SSLv2 の有効/無効

5.4.1　ネットワーク速度の設定

本装置の LAN ポートのネットワーク速度を以下の設定から選択することができます。

- Auto-Negotiate : 接続先とオートネゴシエーションします。
- 10Mbps, Half Duplex : 10Mbps, Half Duplex に固定設定します。
- 10Mbps, Full Duplex : 10Mbps, Full Duplex に固定設定します。
- 100Mpbs, Half Duplex : 100Mbps, Half Duplex に固定設定します。
- 100Mpbs, Full Duplex : 100Mbps, Full Duplex に固定設定します。
- 1000Mbps, Full Duplex : 1000Mbps, Full Duplex に固定設定します。

① 下のような Main Menu 画面において、Enter selection プロンプトに ”1”（Network Configuration）を入力します。

```
+-----------------------------------------------+
|              2x1x16 Switch Console             |
|                                                |
|                 1.18.0.22011                   |
|                                                |
| Copyright (c) 2000-2012, All Rights Reserved   |
+-----------------------------------------------+
|                   Main Menu                    |
+-----------------------------------------------+

     1. Network Configuration
     2. Enable Debug Messages
     3. Reset Appliance
     0. Exit

  Enter selection -> 1 Enter↵
```

② 下のような Network Configuration Menu 画面において、Enter selection プロンプトに ”1”（Network Speed）を入力します。

```
  Enter selection -> 1

+-----------------------------------------------+
|              2x1x16 Switch Console            |
|                                               |
|                  1.18.0.22011                 |
|                                               |
|  Copyright (c) 2000-2012, All Rights Reserved |
+-----------------------------------------------+
|            Network Configuration Menu         |
+-----------------------------------------------+

       MAC Address    [ 00:e0:86:16:78:b5 ]

     1. Network Speed             [ Auto ]
     2. IP Configuration          [ None ]
     6. OBWI Legacy SSLv2 Support [ Disabled ]
     0. Exit/Apply changes

  Enter selection -> 1 Enter↵
```

③ 下のような Network Speed Menu 画面が表示されます。デフォルト設定は、Auto-Negotiate になっています。Enter selection プロンプトに、任意の設定番号を入力します。

```
  Enter selection -> 1

+-----------------------------------------------+
|              1x1x8 Switch Console             |
|                                               |
|                  1.18.0.22011                 |
|                                               |
|  Copyright (c) 2000-2012, All Rights Reserved |
+-----------------------------------------------+
|                Network Speed Menu             |
+-----------------------------------------------+

    1.  Auto-Negotiate
    2.  10 Mbps/Half Duplex
    3.  10 Mbps/Full Duplex
    4.  100 Mbps/Half Duplex
    5.  100 Mbps/Full Duplex
    6.  1000 Mbps/Full Duplex
    0.  Exit without change

  Current Setting  [ Auto ]

  Enter selection -> 6 Enter↵
```

上記の例では 1 ギガビット／全二重 を選択したことになります。

④ 下のように表示されます。任意のキーを入力します。

```
  Enter selection -> 6


Press any key to continue
```

5

シリアルコンソール

⑤ Network Configuration Menu 画面に戻ります。Network Speed 項目の右側の[]内の表示が選択した設定内容に変更されていることを確認します。設定を反映させるために、ここで Enter selection プロンプトに ”0”（Exit/Apply changes）を入力します。

```
+--------------------------------------------------+
|              2x1x16 Switch Console               |
|                                                  |
|                  1.18.0.22011                    |
|                                                  |
|  Copyright (c) 2000-2012, All Rights Reserved    |
+--------------------------------------------------+
|                IP Configuration                  |
+--------------------------------------------------+

       MAC Address    [ 00:e0:86:16:78:b5 ]

     1. Network Speed          [ 1000 Mbps/Full Duplex ]
     2. IP Configuration       [ None ]
     6. OBWI Legacy SSLv2 Support [ Disabled ]
     0. Exit/Apply changes

  Enter selection -> 0 Enter↵
```


⑥ ネットワーク設定変更の確認入力が求められます。変更を保存・適用する場合は、保存確認プロンプトに対して ”yes” を入力します。

```
  Enter selection -> 0

Network configuration changed.  Save? [YES/NO] -> yes Enter↵
```

⑦ 下のように表示され、設定変更が反映されます。

```
Network configuration changed.  Save? [YES/NO] -> yes

Saving network configuration....... Success

Press any key to continue
```

任意のキーを入力すると Main Menu 画面に戻ります。

⑧ <参考> もし上記 6 の場面で “no” を入力するつ、保存せずに終了します。

```
Network configuration changed.  Save? [YES/NO] -> no

Previous network configuration restored

Press any key to continue
```

5.4.2　IP の設定

IP の設定について、以下の設定から選択することができます。

- None　　　　　　　　:　無効
- IPv4 Static　　　　　:　固定 IPv4
- IPv4 DHCP　　　　　:　DHCP IPv4
- IPv6 Static　　　　　:　固定 IPv6
- IPv6 DHCPv6　　　　:　DHCPv6 IPv6

① 下のような Main Menu 画面において、Enter selection プロンプトに ”1”（Network Configuration)を入力します。

```
+-------------------------------------------------+
|              2x1x16 Switch Console              |
|                                                 |
|                  1.18.0.22011                   |
|                                                 |
|  Copyright (c) 2000-2012, All Rights Reserved   |
+-------------------------------------------------+
|                IP Configuration                 |
+-------------------------------------------------+

     1. Network Configuration
     2. Enable Debug Messages
     3. Reset Appliance
     0. Exit

  Enter selection -> 1 Enter↵
```

② 下のような Network Configuration Menu 画面において、Enter selection プロンプトに ”2”（IP Configuration)を入力します。

```
  Enter selection -> 1

+-------------------------------------------------+
|              2x1x16 Switch Console              |
|                                                 |
|                  1.18.0.22011                   |
|                                                 |
|  Copyright (c) 2000-2012, All Rights Reserved   |
+-------------------------------------------------+
|            Network Configuration Menu           |
+-------------------------------------------------+

       MAC Address    [ 00:e0:86:16:78:b5 ]

     1. Network Speed             [ Auto ]
     2. IP Configuration          [ Nonec ]
     6. OBWI Legacy SSLv2 Support [ Disabled ]
     0. Exit/Apply changes

  Enter selection -> 2 Enter↵
```

③ 下のような IP Configuration 画面において、任意の IP 設定を選択し、その項目番号を入力します。

```
Enter selection -> 2

+-----------------------------------------------+
|              2x1x16 Switch Console            |
|                                               |
|                   1.18.0.22011                |
|                                               |
| Copyright (c) 2000-2012, All Rights Reserved  |
+-----------------------------------------------+
|                IP Configuration               |
+-----------------------------------------------+

    1.  None
    2.  IPv4 Static
    3.  IPv4 DHCP
    4.  IPv6 Static
    5.  IPv6 DHCPv6
    0.  Exit without change

Enter selection -> 2 Enter↵
```

ここでは 2 番を選択しています。

④ Network Configuration Menu 画面に戻ります。IP Configuration 項目の右側の[]内の表示が選択した設定内容に変更されていることを確認します。

```
Enter selection -> 2

+-----------------------------------------------+
|              2x1x16 Switch Console            |
|                                               |
|                   1.18.0.22011                |
|                                               |
| Copyright (c) 2000-2012, All Rights Reserved  |
+-----------------------------------------------+
|           Network Configuration Menu          |
+-----------------------------------------------+

     MAC Address    [ 00:e0:86:16:78:b5 ]

    1. Network Speed             [ Auto ]
    2. IP Configuration          [ IPv4 Static ]
    3. IP Address                [ 0.0.0.0 ]
    4. Netmask                   [ 0.0.0.0 ]
    5. Default Gateway           [ none ]
    6. OBWI Legacy SSLv2 Support [ Disabled ]
    0. Exit/Apply changes

Enter selection ->
```

前のステップで 2 番を選択したことにより IPv4 が有効になり、隠れていた設定項目が表示されています。(3～5 番)。
固定の IP アドレスを設定する場合には、次項の「IP アドレスの設定」を実行します。
この状態で設定を反映させることはできませんので、次項に進んでください。

5.4.3 IP アドレスの設定

本装置のシリアルコンソールポートからネットワーク設定することができます。IP アドレスの設定手順について説明します。

以下のような、固定の IP アドレスを設定する場合の例を示します。

IP アドレス	:	192.168.1.100
サブネットマスク:	:	255.255.255.0
デフォルトゲートウェイ:	:	192.168.1.1

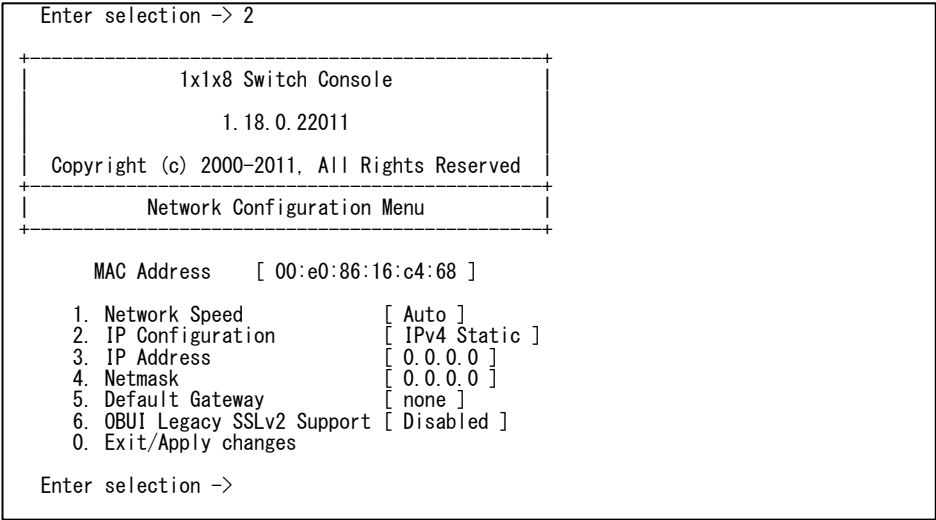
① 前項の続きに戻ります。

```
  Enter selection -> 2

+------------------------------------------------+
|              1x1x8 Switch Console              |
|                                                |
|                  1.18.0.22011                  |
|                                                |
|  Copyright (c) 2000-2011, All Rights Reserved  |
+------------------------------------------------+
|           Network Configuration Menu           |
+------------------------------------------------+

       MAC Address    [ 00:e0:86:16:c4:68 ]

     1. Network Speed            [ Auto ]
     2. IP Configuration         [ IPv4 Static ]
     3. IP Address               [ 0.0.0.0 ]
     4. Netmask                  [ 0.0.0.0 ]
     5. Default Gateway          [ none ]
     6. OBUI Legacy SSLv2 Support [ Disabled ]
     0. Exit/Apply changes

  Enter selection ->
```

② IP アドレスを設定します。Enter selection プロンプトに ”3”（IP Address）を入力します。

```
  Enter selection -> 3 Enter↵
```

③ Enter IP address プロンプトが表示されるので、任意の IP アドレスを入力します（下の例では、192.168.1.100 に設定しています）。

```
Enter IP address -> 192.168.1.100 Enter↵
```

④ 再び Enter selection プロンプトに制御が戻ります。IP Address 項目の右側の[ ]内に設定値が入ります。

```
Enter IP address -> 192.168.1.100

+--------------------------------------------------+
|               2x1x16 Switch Console              |
|                                                  |
|                   1.18.0.22011                   |
|                                                  |
|  Copyright (c) 2000-2012, All Rights Reserved    |
+--------------------------------------------------+
|             Network Configuration Menu           |
+--------------------------------------------------+

       MAC Address     [ 00:e0:86:16:78:b5 ]

     1. Network Speed             [ Auto ]
     2. IP Configuration          [ IPv4 Static ]
     3. IP Address                [ 192.168.1.100 ]
     4. Netmask                   [ 0.0.0.0 ]
     5. Default Gateway           [ none ]
     6. OBWI Legacy SSLv2 Support [ Disabled ]
     0. Exit/Apply changes

  Enter selection ->
```

⑤ 続いてネットマスクを設定します。Enter selection プロンプトに ”4” （Netmask）を入力します。

```
  Enter selection -> 4 Enter↵
```

⑥ Enter subnet mask プロンプトが表示されるので、任意の値を入力します（下の例では、255.255.255.0 に設定しています）。

```
Enter subnet mask -> 255.255.255.0 Enter↵
```

⑦ 再び Enter selection プロンプトに制御が戻ります。Netmask 項目の右側の[ ]内に設定値が入ります。

```
Enter subnet mask -> 255.255.255.0

+--------------------------------------------------+
|               2x1x16 Switch Console              |
|                                                  |
|                   1.18.0.22011                   |
|                                                  |
|  Copyright (c) 2000-2012, All Rights Reserved    |
+--------------------------------------------------+
|             Network Configuration Menu           |
+--------------------------------------------------+

       MAC Address     [ 00:e0:86:16:78:b5 ]

     1. Network Speed             [ Auto ]
     2. IP Configuration          [ IPv4 Static ]
     3. IP Address                [ 192.168.1.100 ]
     4. Netmask                   [ 255.255.255.0 ]
     5. Default Gateway           [ none ]
     6. OBWI Legacy SSLv2 Support [ Disabled ]
     0. Exit/Apply changes

  Enter selection ->
```

⑧ 続いてデフォルトゲートウェイを設定します。Enter selection プロンプトに ”5”（Default Gateway）を入力します。

```
  Enter selection -> 5 Enter↵
```

⑨ Enter default gateway IP address プロンプトが表示されるので、任意の値を入力します（下の例では、192.168.1.1 に設定しています）。

```
Enter "0.0.0.0" to remove default gateway

Enter default gateway IP address -> 192.168.1.1 Enter↵
```

⑩ 再び Enter selection プロンプトに制御が戻ります。Default Gateway 項目の右側の[]内に設定値が入ります。

```
Enter default gateway IP address -> 192.168.1.1

+------------------------------------------------+
|              2x1x16 Switch Console             |
|                                                |
|                  1.18.0.22011                  |
|                                                |
|  Copyright (c) 2000-2012, All Rights Reserved  |
+------------------------------------------------+
|           Network Configuration Menu           |
+------------------------------------------------+

       MAC Address    [ 00:e0:86:16:78:b5 ]

     1. Network Speed              [ Auto ]
     2. IP Configuration           [ IPv4 Static ]
     3. IP Address                 [ 192.168.1.100 ]
     4. Netmask                    [ 255.255.255.0 ]
     5. Default Gateway            [ 192.168.1.1 ]
     6. OBWI Legacy SSLv2 Support  [ Disabled ]
     0. Exit/Apply changes

  Enter selection ->
```

⑪ 設定が終了したら、設定を反映させるために Enter selection プロンプトに ”0”（Exit/Apply changes）を入力します。

```
  Enter selection -> 0 Enter↵
```

⑫ 変更を保存・適用する場合は、保存確認プロンプトに対して ”yes” を入力します。

```
  Enter selection -> 0


Network configuration changed.  Save? [YES/NO] -> yes Enter↵
```

⑬ 下のように表示され、設定変更が反映されます。

```
Network configuration changed.  Save? [YES/NO] -> yes

Saving network configuration....... Success

Press any key to continue
```

以上のような手順で ネットワークに関する設定変更を行なうことができます。

5.4.4　OBWI における SSL 設定

OBWI における、SSL version2 のサポートの有効/無効を設定することができます。

① 下のように Network Configuration Menu 画面において、Enter selection プロンプトに ”6”（OBWI Legacy SSLv2 Support）を入力します。

```
+----------------------------------------------+
|               2x1x16 Switch Console          |
|                                              |
|                   1.18.0.22011               |
|                                              |
|  Copyright (c) 2000-2012, All Rights Reserved |
+----------------------------------------------+
|           Network Configuration Menu         |
+----------------------------------------------+

      MAC Address    [ 00:e0:86:16:78:b5 ]

    1. Network Speed              [ Auto ]
    2. IP Configuration           [ IPv4 Static ]
    3. IP Address                 [ 192.168.1.100 ]
    4. Netmask                    [ 255.255.255.0 ]
    5. Default Gateway            [ 192.168.1.1 ]
    6. OBWI Legacy SSLv2 Support  [ Disabled ]
    0. Exit/Apply changes

  Enter selection -> 6 Enter↵
```

② 下のような確認プロンプトに対して、SSL version2 を有効にする場合は、”yes” を入力します。（無効にする場合は、”no” を入力します。）

```
  Enter selection -> 6

Allow unsecure legacy SSLv2 for OBWI? [YES/NO] -> yes Enter↵
```

③ 下のように OBWI Legacy SSLv2 Support 項目の右側の[ ]内の表示が ”Enabled” と表示されます。

```
Allow unsecure legacy SSLv2 for OBWI? [YES/NO] -> yes

+----------------------------------------------+
|               1x1x8 Switch Console           |
|                                              |
|                   1.18.0.22011               |
|                                              |
|  Copyright (c) 2000-2011, All Rights Reserved |
+----------------------------------------------+
|           Network Configuration Menu         |
+----------------------------------------------+

      MAC Address    [ 00:e0:86:16:c4:68 ]

    1. Network Speed              [ Auto ]
    2. IP Configuration           [ IPv4 Static ]
    3. IP Address                 [ 192.168.1.100 ]
    4. Netmask                    [ 255.255.255.0 ]
    5. Default Gateway            [ 192.168.1.1 ]
    6. OBWI Legacy SSLv2 Support  [ Enabled ]
    0. Exit/Apply changes

  Enter selection ->
```

④ 設定が終了したら、設定を反映させるために Enter selection プロンプトに ”0”（Exit/Apply changes）を入力します。

```
  Enter selection -> 0 Enter↵
```

⑤ 変更を保存・適用する場合は、保存確認プロンプトに対して ”yes” を入力します。

```
  Enter selection -> 0

Network configuration changed.  Save? [YES/NO] -> yes Enter↵
```

⑥ 下のように表示され、設定変更が反映されます。

```
Network configuration changed.  Save? [YES/NO] -> yes
Saving network configuration....... Success
OBWI Legacy SSLv2 is now Enabled
Press any key to continue
```

5.5. デバッグメッセージの有効化

本装置のシリアルコンソールポートからデバッグメッセージを出力させることができます。

① 下のような Main Menu 画面において、Enter selection プロンプトに ”2”（Enable Debug Messages）を入力します。

```
+-------------------------------------------------+
|              1x1x8 Switch Console               |
|                                                 |
|                   1.18.0.22011                  |
|                                                 |
|  Copyright (c) 2000-2012, All Rights Reserved   |
+-------------------------------------------------+
|                    Main Menu                    |
+-------------------------------------------------+

     1. Network Configuration
     2. Enable Debug Messages
     3. Reset Appliance
     0. Exit

  Enter selection -> 2 Enter↵
```

② 下のように表示され、デバッグメッセージの出力が有効な状態になります。

```
  Enter selection -> 2

Press any key to disable debug messages
  and return to Console Menu
```

任意のキー入力を行うとデバッグメッセージの出力は無効となり、再び Main Menu 画面に戻ります。

デバッグメッセージの出力を有効にすると本装置のパフォーマンスが大きく低下することがあるため、弊社サポートによる指示など、どうしても必要な場合にのみ有効にしてください。

5.6. 再起動

シリアルコンソールから本装置を再起動する手順について説明します。

① Main Menu 画面において、Enter selection プロンプトに ”3”（Reset Appliance)を入力します。

```
+-----------------------------------------------+
|              2x1x16 Switch Console            |
|                                               |
|                   1.18.0.22011                |
|                                               |
|  Copyright (c) 2000-2012, All Rights Reserved |
+-----------------------------------------------+
|                    Main Menu                  |
+-----------------------------------------------+

    1. Network Configuration
    2. Enable Debug Messages
    3. Reset Appliance
    0. Exit

 Enter selection -> 3 Enter↵
```

② 再起動を実行する場合は、再起動確認プロンプトに対して ”yes” を入力します。

```
+-----------------------------------------------+
|              2x1x16 Switch Console            |
|                                               |
|                   1.18.0.22011                |
|                                               |
|  Copyright (c) 2000-2012, All Rights Reserved |
+-----------------------------------------------+
|                    Main Menu                  |
+-----------------------------------------------+

    1. Network Configuration
    2. Enable Debug Messages
    3. Reset Appliance
    0. Exit

 Enter selection -> 3


Reset 1x1x8 Switch? [YES/NO] -> yes Enter↵
```

③ 下のように表示され、再起動が実行されます。

```
Reset 2x1x16 Switch? [YES/NO] -> yes


Resetting to activate changes.
This will require approximately one minute...
```

以上で、再起動の手順は完了です。約 1 分 30 秒後、本装置は起動します。

5.7. ログインパスワードの入力

OBWI の「ポート設定のセットアップ」ページにおいて、"ポート セキュリティのセットアップを有効にする" にチェックを入れ、任意のパスワード設定を行うことにより、シリアルコンソールにログインするためのセキュリティ設定を有効にすることができます。

📖 参照 3.23 セットアップポートの設定（127 ページ）

① セキュリティ設定が有効になっている場合、下のように "Enter password" プロンプトが表示され、シリアルコンソールアクセス時にパスワード入力が要求されます。

```
Security Active -- Please login

If password is lost, type "HELP" at password prompt
to begin procedure to unlock appliance.


Enter password:
```

② 設定したパスワードを入力します。

```
Enter password: ***** Enter↵
```

③ パスワード認証に成功すると、Main Menu 画面が表示されます。

```
Enter password: *****

+-------------------------------------------------+
|               2x1x16 Switch Console             |
|                                                 |
|                   1.18.0.22011                  |
|                                                 |
|  Copyright (c) 2000-2012, All Rights Reserved   |
+-------------------------------------------------+
|                    Main Menu                    |
+-------------------------------------------------+

     1. Network Configuration
     2. Enable Debug Messages
     3. Reset Appliance
     0. Exit

  Enter selection ->
```

5.8. ブートメニューの実行

本装置の起動途中に任意のキーを入力することにより、ブートメニューを表示させることができます。ブートメニューでは、起動ファームウェアの選択、設定の初期化などを実行することができます。

ブートメニューの実行手順について下記に説明します。

① 本装置の電源をオンすると直後に下のように表示されます。"Hit any key to stop autoboot:" という文字列が表示されてから約 3 秒間の間に任意のキーを入力します。

```
U-Boot version:U-Boot 1.3.0-rc3 (Feb 22 2013 - 16:07:52) Polaris 2.1.20060


AVODSR
Serial Number:0013070000
EID:520594-001307-0000
MAC Addr 1:00:e0:86:16:78:b5
MAC Addr 2:00:e0:86:16:78:b6
Current Firmware Version  :1.18.0.22011
Alternate Firmware Version:1.18.0.22011
Hit any key to stop autoboot:+++          ← ここで任意のキー入力
```

② 下のようなブートメニューが表示されます。キー入力が間に合わず本装置がブート状態に入ってしまった場合は、再度本装置を再起動し、"Hit any key to stop autoboot:" が表示されるタイミングでキー入力を行ってください。

```
Hit any key to stop autoboot:++
=================================
0) Boot Current.[1.18.0.22011]
1) Boot Alternate.[1.18.0.22011]
2) Configuration Reset.
3) Factory Reset.
Enter Number to Select Option:>
```

約 20 秒間コマンドの入力がない場合、タイムアウトとなり、再起動されます。
ブートメニューのコマンドについて下記に説明します。

ブートメニュー コマンド内容

番号	設定内容	🕮 参照
0	通常起動。"Boot Current." 表示の右側[]内のファームウェアバージョンで起動します。	240 ページ
1	代替ファームウェアでの起動。"Boot Alternate." 表示の右側[]内のファームウェアバージョンで起動します。	241 ページ
2	本装置の全ての設定値を削除します。	242 ページ
3	工場出荷時の状態にリセットします。本装置の全ての設定値を初期化し、ファームウェアをリロードします。	243 ページ

各コマンドの詳細については、次項から説明します。

5.8.1　通常起動

ブートメニューにおいて、通常起動する手順を説明します。

① 本装置の起動時に任意のキーを入力して、ブートメニューを表示させせます。
参照 5.8 ブートメニューの実行（239 ページ）

② 下のようなブートメニューにおいて、"0" を入力します。

```
Hit any key to stop autoboot:++
=================================
0) Boot Current.[ 1.18.0.22011]
1) Boot Alternate.[ 1.18.0.22011]
2) Configuration Reset.
3) Factory Reset.
Enter Number to Select Option:> 0
```

③ 下のように、通常起動状態に戻ります。約 1 分で本装置は起動します。

```
Enter Number to Select Option: > 0
Rebooting...

U-Boot version:U-Boot 1.3.0-rc3 (Feb 22 2013 - 16:07:52) Polaris 2.1.20060


AVODSR
Serial Number:0013070000
EID:520594-001307-0000
MAC Addr 1:00:e0:86:16:78:b5
MAC Addr 2:00:e0:86:16:78:b6
Current Firmware Version  :1.18.0.22011
Alternate Firmware Version:1.18.0.22011
Hit any key to stop autoboot::+++

Booting: 1.18.0.22011
```

5.8.2　代替ファームウェアでの起動

ブートメニューにおいて、代替ファームウェアで起動する手順を説明します。
本装置が正常に起動しない場合などに、復旧手段として代替ファームウェアで起動させることができます。"Boot Alternate." 表示の右側の[]内に代替ファームウェアのバージョンが表示されています。

① 本装置の起動時に任意のキーを入力して、ブートメニューを表示させせます。
📖 参照 5.8 ブートメニューの実行（239 ページ）

② 下のようなブートメニューにおいて、"1" を入力します。

```
Hit any key to stop autoboot:++
=================================
0) Boot Current.[1.18.0.22011]
1) Boot Alternate.[1.18.0.22011]
2) Configuration Reset.
3) Factory Reset.
Enter Number to Select Option:> 1
```

③ 下のように、確認入力が求められます。代替ファームウェアで起動させる場合は、"y" を入力します。

```
Enter Number to Select Option:> 1
Are you sure? [Y/N]:y
```

④ 代替ファームウ ェアでの起動が始まります。約 1 分で本装置は起動します。

```
Are you sure? [Y/N]:>y
Rebooting...

U-Boot version:U-Boot 1.3.0-rc3 (Feb 22 2013 - 16:07:52) Polaris 2.1.20060


AVODSR
Serial Number:0013070000
EID:520594-001307-0000
MAC Addr 1:00:e0:86:16:78:b5
MAC Addr 2:00:e0:86:16:78:b6
Current Firmware Version  :1.18.0.22011
Alternate Firmware Version:1.18.0.22011
Hit any key to stop autoboot::+++

Booting: 1.18.0.22011
```

5.8.3　設定値の削除

ブートメニューにおいて、設定値を削除する手順を説明します。
本操作を実行するとIPアドレスなど全ての設定値がリセットされます。

① 本装置の起動時に任意のキーを入力して、ブートメニューを表示させます。
参照 5.8 ブートメニューの実行（239ページ）

② 下のようなブートメニューにおいて、"2" を入力します。

```
Hit any key to stop autoboot:++
=================================
0) Boot Current.[1.18.0.22011]
1) Boot Alternate.[1.18.0.22011]
2) Configuration Reset.
3) Factory Reset.
Enter Number to Select Option:> 2
```

③ 下のように、確認入力が求められます。設定値を削除する場合は、"y" を入力します。

```
Enter Number to Select Option:>2
Are you sure? [Y/N]:y
```

④ 通常起動し、設定値が削除されます。

```
Are you sure? [Y/N]:>y
Rebooting...

U-Boot version:U-Boot 1.3.0-rc3 (Feb 22 2013 - 16:07:52) Polaris 2.1.20060


AVODSR
Serial Number:0013070000
EID:520594-001307-0000
MAC Addr 1:00:e0:86:16:78:b5
MAC Addr 2:00:e0:86:16:78:b6
Current Firmware Version  :1.18.0.22011
Alternate Firmware Version:1.18.0.22011
Hit any key to stop autoboot::+++

Booting: 1.18.0.22011
(以下省略)
```

5.8.4　工場出荷状態への初期化

ブートメニューにおいて、本装置を工場出荷時の状態へ初期化する手順を説明します。

① 本装置の起動時に任意のキーを入力して、ブートメニューを表示させます。
参照 5.8 ブートメニューの実行（239 ページ）

② 下のようなブートメニューにおいて、”3” を入力します。

```
Hit any key to stop autoboot:++
=================================
0) Boot Current.[1.18.0.22011]
1) Boot Alternate.[1.18.0.22011]
2) Configuration Reset.
3) Factory Reset.
Enter Number to Select Option:> 3
```

③ 下のように、確認入力が求められます。出荷状態へ初期化させる場合は、”y” を入力します。

```
Enter Number to Select Option:>3
Are you sure? [Y/N]:y
```

④ 設定値の初期化後、ファームウェアが再読み込みされて起動します。

```
Are you sure? [Y/N]:>y
Rebooting...

U-Boot version:U-Boot 1.3.0-rc3 (Feb 22 2013 - 16:07:52) Polaris 2.1.20060


AVODSR
Serial Number:0013070000
EID:520594-001307-0000
MAC Addr 1:00:e0:86:16:78:b5
MAC Addr 2:00:e0:86:16:78:b6
Current Firmware Version  :1.18.0.22011
Alternate Firmware Version:1.18.0.22011
Hit any key to stop autoboot::+++

Booting: 1.18.0.22011
(以下省略)
```

Chapter 6 - 諸元

本製品の仕様について説明しています。

本章の内容

6.1. 本製品の仕様

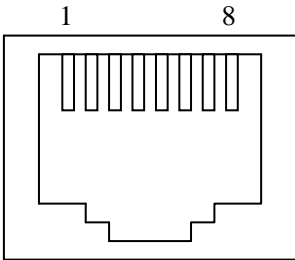
項目		仕様		
シリーズ名		SERVIS IP-KVM FW-D シリーズ		
型格		FW-D1108NP	FW-D2116NP	FW-D8132NP
ターゲット ポート	ポート数	8	16	32
	解像度 *3	640 × 480 (60Hz) 800 × 500 (60Hz) 800 × 600 (75Hz) 960 × 700 (75Hz) 1024 × 768 (75Hz) 1024 × 640 (60Hz) 1280 × 1024 (75Hz) *1 1280 × 800 (60Hz) *2 1440 × 900 (60Hz) *2 1600 × 1200 (60Hz) *2 1680 × 1050 (60Hz) *2 *1・・・FW-DSM02/PS2-M, FW-DSM02/USB-L を使用時、ビデオセッションビューアの表示解像度は 1024 x 768 超には設定できません。 *2・・・FW-DSM03/VMC のみ対応します。		
	信号種	VESA RGB 信号、コンポジット信号非対応、DDC2B 対応		
	入出力 I/F	PS/2 (キーボード、マウス)、USB (キーボード、マウス、ストレージ)、RS-232C シリアル		
LAN ポート	ポート数	2		
	タイプ	10/100/1000 BASE-T Ethernet		
	IP バージョン	IPv4, IPv6		
	データレート	最大 20Mbps		
USB ポート	ポート数	4		
	規格タイプ	USB2.0 (High Speed には未対応)		
	接続可能機器	HID 規定キーボード、HID 規定マウス、USB CD/DVD ドライブ、USB Flash Disk、USB フロッピーディスクドライブ		
PDU ポート	ポート数	2		
	コネクタ	RJ45		
	タイプ	本機独自 (信号は RS-232C 互換)		
	通信設定	9600bps, 8bit, non parity, 1 stop bit, no flow		
SETUP ポート	ポート数	1		
	コネクタ	RJ45		
	タイプ	RS-232C シリアル		
	通信設定	9600bps, 8bit, non parity, 1 stop bit, no flow		
MODEM ポート	ポート数	1		
	コネクタ	RJ45		
	タイプ	RS-232C シリアル		
	通信設定	9600bps, 8bit, non parity, 1 stop bit, no flow		
カスケード ポート	ポート数	1		
	コネクタ	RJ45		
モニター ポート	ポート数	1		
	コネクタ	D-Sub 15pin(DE15)		
	タイプ	VESA 準拠		
電源	ポート数	2 (冗長構成)		
	入力定格	AC 100V～240V, 50Hz/60Hz, 1.25A		
	消費電力(max)	13W	18W	24W
外形寸法 [mm]	高さ 幅 奥行き	43.7 430.0 234.3		43.7 430.0 336.1
質量(本体のみ)		3.1kg	3.2kg	3.9kg

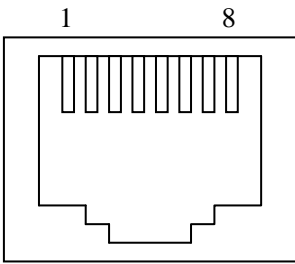
*3・・・サポートするケーブルは、CAT5e または CAT6 のストレートで 45m 以内です。

6.2. 環境条件

項目	
周囲温度	動作時: 0～50℃ 保存時: -20～70℃
周囲湿度	動作時: 20～80%RH（結露なきこと） 保存時: 5～95%RH、最大湿球温度 38.7℃ 温度条件: 38.7℃以下で 95%RH 上限
適合規格	UL, FCC, cUL, ICES-003, CE, VCCI

6.3. コネクタのピン配列

6.3.1 SETUP ポートコネクタ

ピン番号	信号名	IN/OUT
1	RTS	OUT
2	DSR	IN
3	DCD	IN
4	RxD	IN
5	TxD	OUT
6	SG	---
7	DTR	OUT
8	CTS	IN

6.3.2 MODEM コネクタ

ピン番号	信号名	IN/OUT
1	N/C	---
2	N/C	---
3	N/C	---
4	RxD	IN
5	TxD	OUT
6	SG	---
7	N/C	---
8	N/C	---

6.4. 使用 TCP ポート

本装置において、使用する TCP ポートの各番号およびその機能を以下に示します。

TCP ポート番号	タイプ	機能・用途
22	SSH	サーバーユニット FW-DSM03/SRL へのシリアルセッションに使用されます。
23	Telnet	サーバーユニット FW-DSM03/SRL へのシリアルセッションに使用されます（Telnet が有効の場合）。
80	HTTP	OBWI 通信に使用されます。
443	HTTPS	OBWI 通信に使用されます。
2068	専用仕様	KVM セッションデータ（マウス、キーボードデータ）の伝送、およびビデオデータの伝送に使用されます。 バーチャルメディアデータの伝送に使用されます。

6.5. 製品サポートについて

<製品に関するお問い合わせ>

富士通コンポーネント株式会社
第二マーケティング部
TEL: 03-5449-7006, FAX: 03-5449-2628
e-mail: promothq@fcl.fujitsu.com
ホームページ: http://www.fcl.fujitsu.com/

<修理・不具合に関するお問い合わせ>

富士通コンポーネント　お客様サービス＆サポートセンター
TEL: 0120-810225　＊携帯, PHS からもご利用になれます。
e-mail: servis-center@fcl.fujitsu.com
営業時間: 9:00〜12:00、13:00〜17:00（土，日，祝祭日を除く）

SERVIS IP-KVM 2nd バージョン
取扱説明書 (KM80-13007-02)

2013 年 8 月発行

富士通コンポーネント株式会社
〒141-8530 東京都品川区東五反田 2-3-5 五反田中央ビル

本書の記載内容は予告無しに変更する事があります。
本書に記載された情報、図面の仕様に起因する第三者の知的財産権、その他権利侵害については、当社はその責を負いません。
本書に記載された製品を使用した貴社製品が、「外国為替及び外国貿易法」ならびに「米国輸出管理規制(EAR)」などの法令に基づき規制されている貨物又は技術に該当する場合に、該当製品を輸出するに際しては同法に基づく許可が必要になります。

落丁、乱丁のあるものはお取り替え致します。